MyPBX Security Configuration Guide

Version: V1.1

Date: Sep., 2013

Contents

VoIP attack, although not an everyday occurrence does exist. When using VoIP, system security is undoubtedly one of the issues we care about most. But with the appropriate configuration, and some basic safety habits, we can improve the security of the telephone system. Moreover, the powerful built-in firewall function in MyPBX is adequate to enable the system to run safely and stably.

This guide will introduce the highest defense level in MyPBX, and we strongly recommend that you configure firewall and other security options according to this guide, to prevent the attack fraud and the system failure or calls loss.

Note:

1. In this guide, the configuration options marked with "*" only exist in X.18.XX.XX and above versions.
2. We recommend upgrading the firmware to the latest edition for security purpose.
3. Don't map any port to MyPBX in router if not needed.
4. We recommend limiting the credit of VoIP trunks for international calls.

Security Center*

Security center is a new feature since x.18.0.xx, we can get an overview of basic settings like firewall, service securty and port guard.

Click "System→ System Preferences→Security Center" to get the details. You can click the button to configure those one by one. You can follow the steps in this manual to configure and get the resut in this page.

1. Port:

This page shows the SIP port and HTTP port, we can click "Setting" to change that. It's recommend that the default port should be changed.

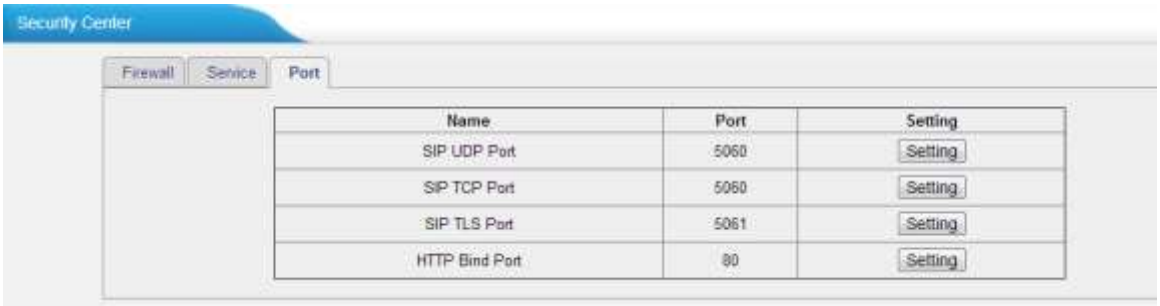


Figure 0-1

2. Service:

This page shows the general service like AMI, SSH and TFTP, we recommend disabling them if not used.

Note: TFTP is used for phone provisioning, it's enabled by default, you can disable it after all phones are well configured.

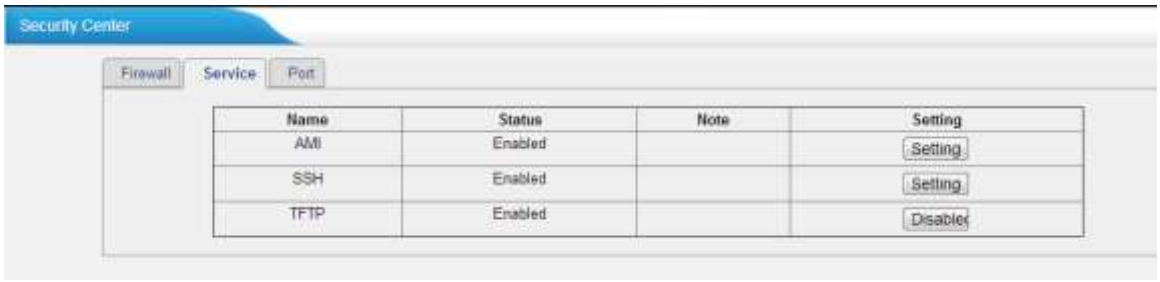


Figure 0-2

3. Firewall:

In this page, the basic information of firewall rules are displayed. We recommend configuring it step by step following part 2 of this manual.

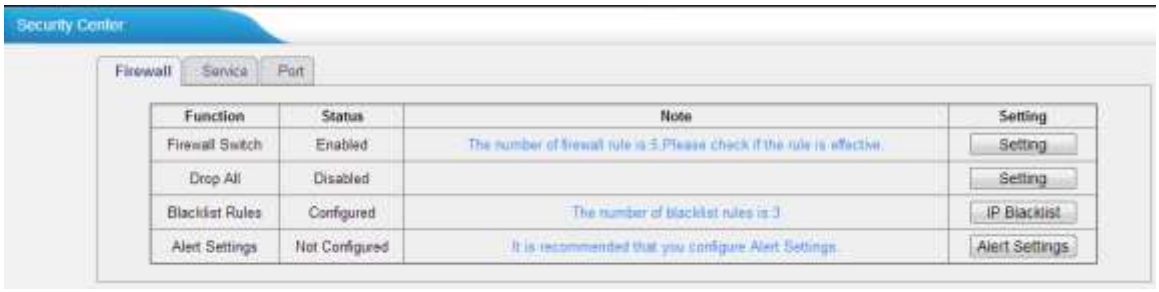


Figure 0-3

1. Ports and password enhancement

Ports and password are most important for security; we recommend changing the default ones to your own.

1.1 Web GUI (HTTP)

1.1.1 Change the default HTTP bind port.

PBX→Basic Settings→ General Preferences→HTTP Bind Port

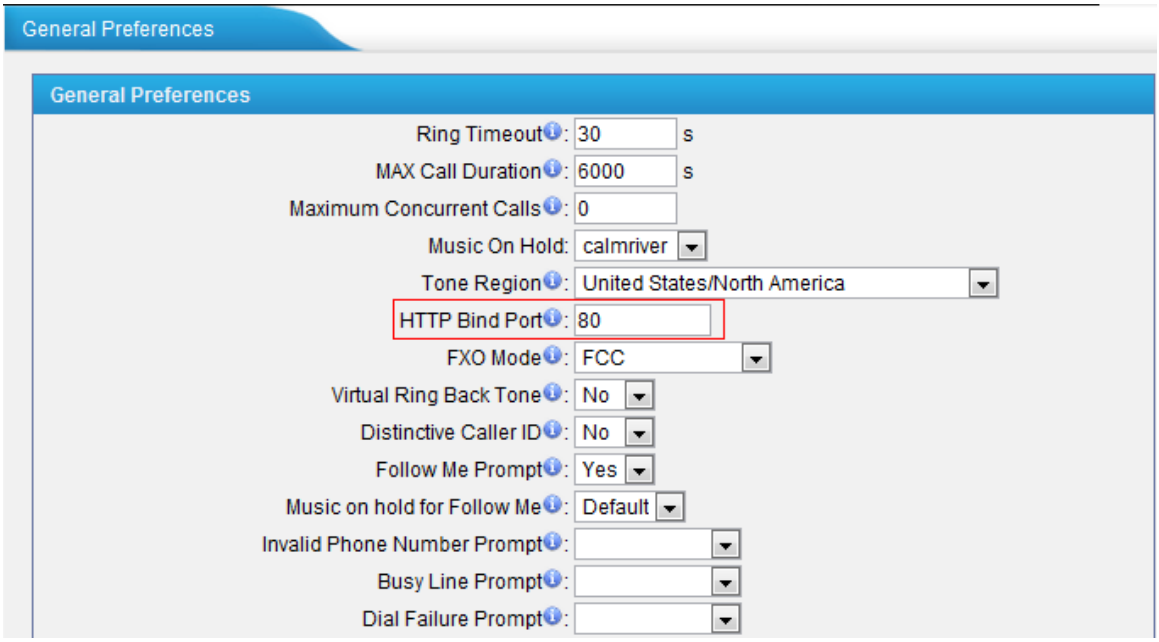


Figure 1-1

We can change it to another one like 8080 for example.

1.1.2 Change the default password.

System→ System Preferences→Change Password

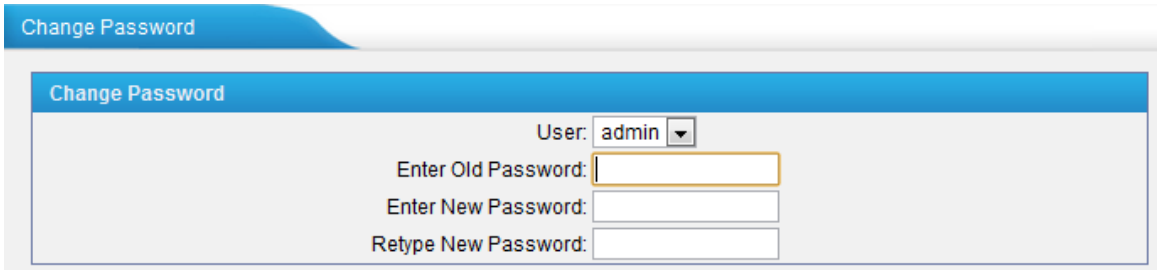


Figure1-2

A strong password needs to be configured here for all accounts. Especially account "admin" and "user".

1.2 Extension

Hackers are always sending packages to PBX to register extension before dialing out. Extension's security is very important for users.

1.2.1 Change the default SIP Port

PBX→Basic settings→SIP Settings→General→UDP Port

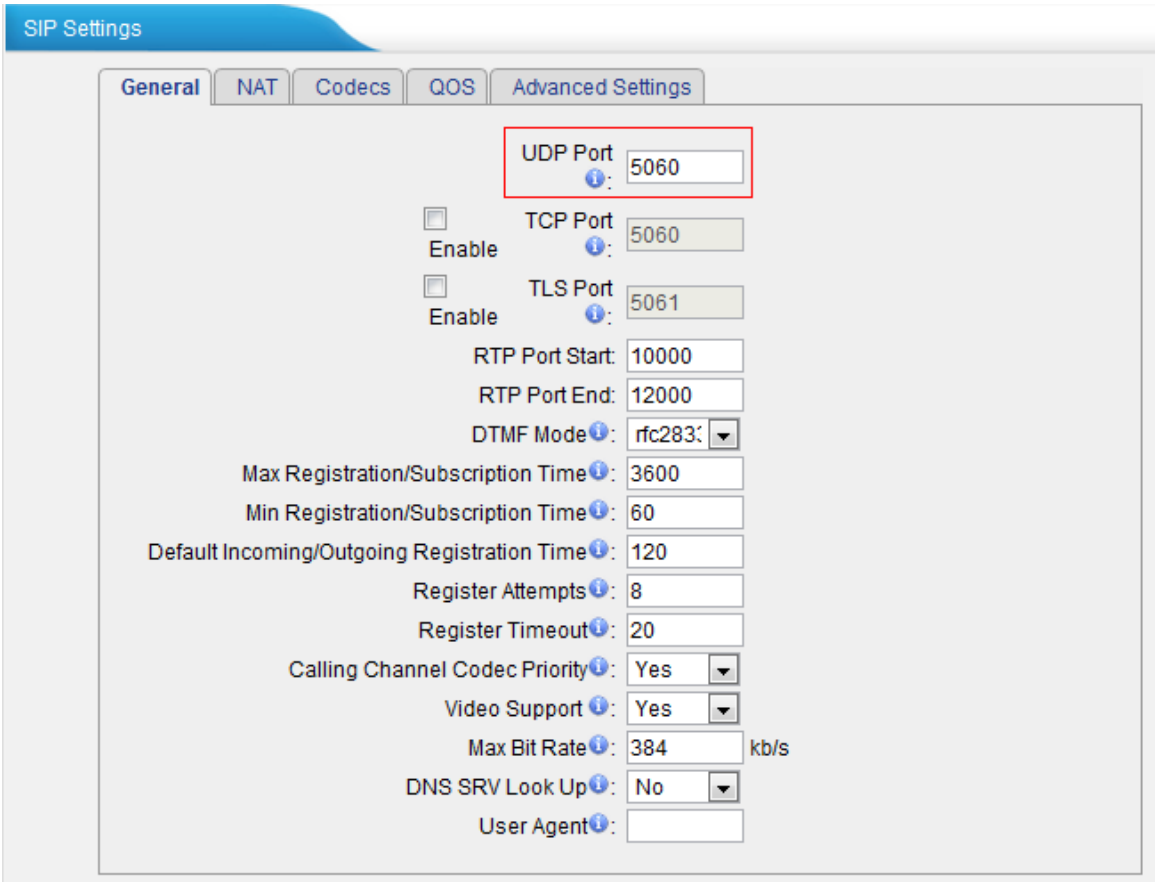


Figure 1-3

We recommend changing this to another available port, for example: 5080.

1.2.2 Change the default password

The password of the extensions is "pincode + extension number". A password with upper and lower letters and numbers is recommended. For example: AjK5Up1G.

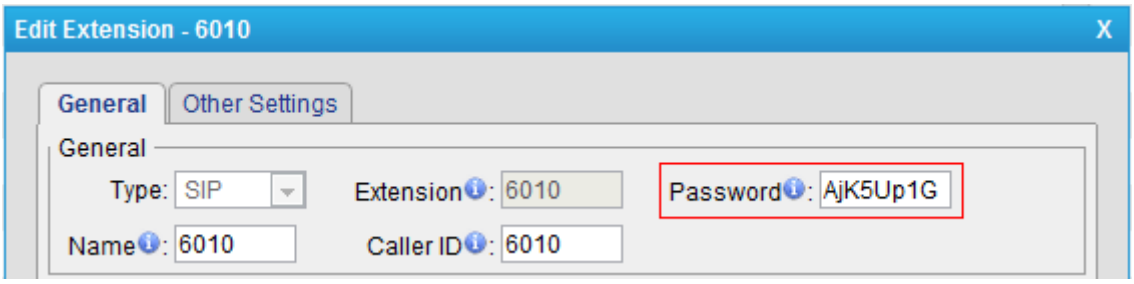


Figure 1-4

Note: A strong password is a MUST for remote extensions.

1.2.3. IP restriction for extensions

You can find this setting in
PBX→Extensions→FXS/VoIP Extensions→ VoIP Extensions→General→Password
When it's configured, only the permitted IP can register this extension. All the other registry requests will be denied.

The format is "IP address/Subnet mask", e.g. 192.168.5.136/255.255.255.255. In this way, only 192.168.5.136 can register this extension 6010.

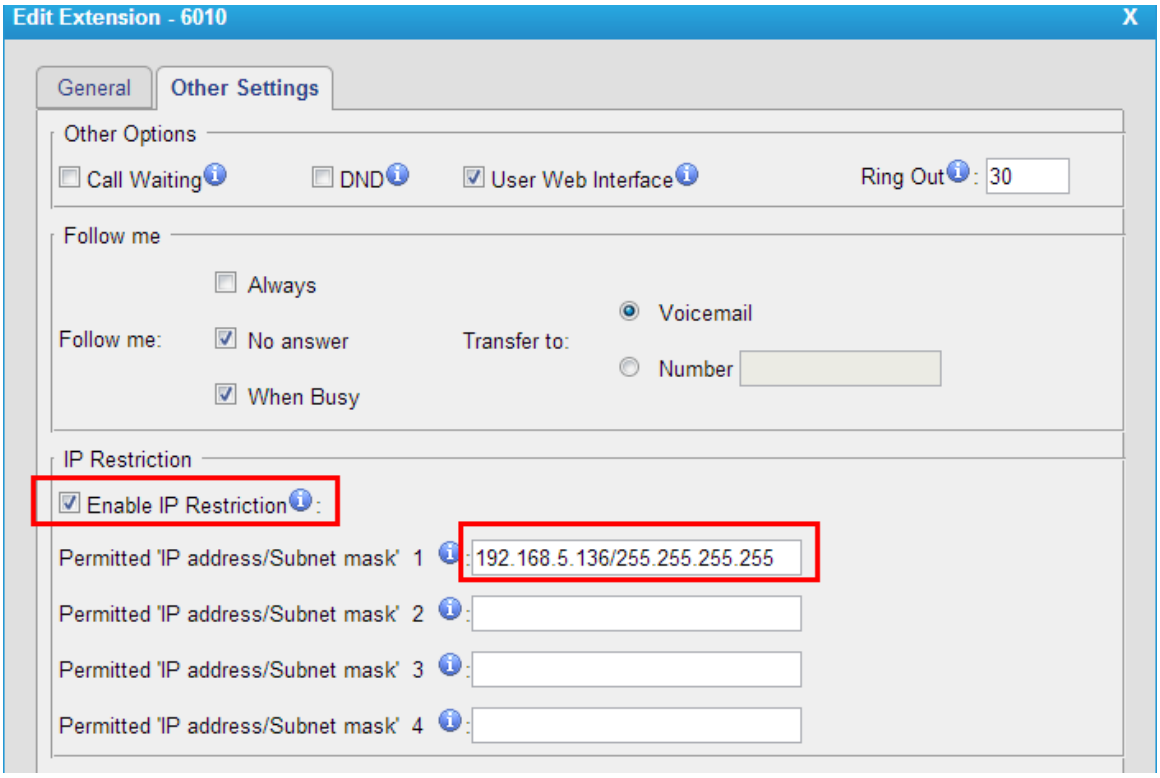


Figure 1-5

Note: If it's for remote extension, a static public IP address is needed to input instead.

1.2.3 Security Configuration for Remote Extensions

PBX→Extensions→FXS/VoIP Extensions→ VoIP Extensions→General
Enable "NAT" and "Register remotely" like the picture shown below.

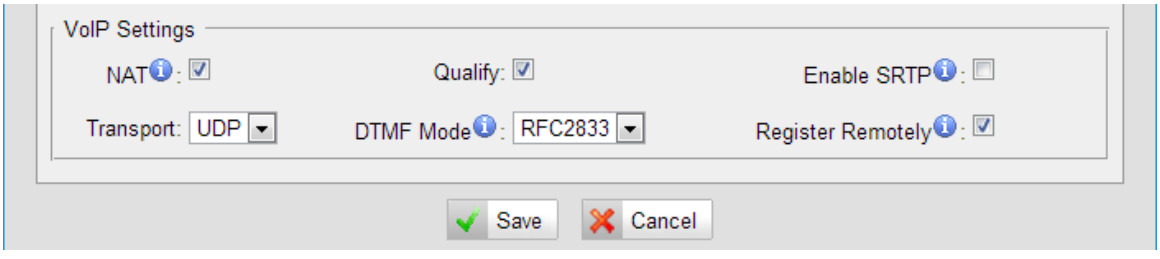


Figure 1-6

Note:
1. If remote registration isn't required, please disable it.
2. If extensions register to MyPBX via WAN port, please only enable "register remotely".

1.2.4 TLS registry (Optional)

Introduction

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide communication security over the Internet. They use asymmetric cryptography for authentication of key exchange, symmetric encryption for confidentiality and message authentication codes for message integrity. Several versions of the protocols are in widespread use in applications such as web browsing, electronic mail, Internet faxing, instant messaging and Voice-over-IP (VoIP).

TLS is supported in MyPBX for security SIP registry; you can also register SIP trunks to VoIP providers via TLS. We need to upload the certificate into MyPBX and the IP phones together for authorization.

Hackers send the register request to PBX for registry via UDP generally, if it's TLS enabled in MyPBX, hacker cannot register extension without the CA, the registry request will be refused directly.

Refer to **Appendix I** to get the detailed steps of how to use TLS in MyPBX.

Note: TLS is disabled in MyPBX by default; we need to enable it in "SIP settings" page in advance before using it.

2. Firewall configuration

Note: Please back up the configurations on Backup and Restore page before you go ahead. In the case that you lock the device, you can reset to factory default and restore the previous configurations. The example rules below work with MyPBX firmware version 2.15.xx.xx or higher versions.

The basic logic to configure firewall is "Allow all trusted IP addresses and then enable 'Drop All'".

Step1. Enable firewall on firewall page of MyPBX.

System→Firewall Settings → Firewall Rules→General Settings

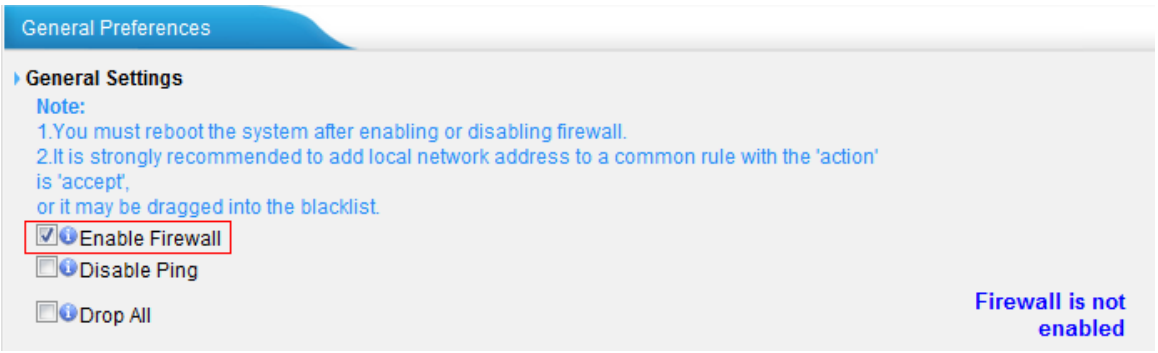


Figure 2-1

Step2. Add common rules to accept local network access.

Create a common rule to allow all the IP addresses of the local phones to access MyPBX server. For example, the local IP range is 192.168.5.1-192.168.5.254, the configuration could be as below:

Name: LocalNetwork
Protocol: BOTH
Port: 1:65535
IP: 192.168.5.0/255.255.255.0, the format must be "IP/net mask"
Action: Accept

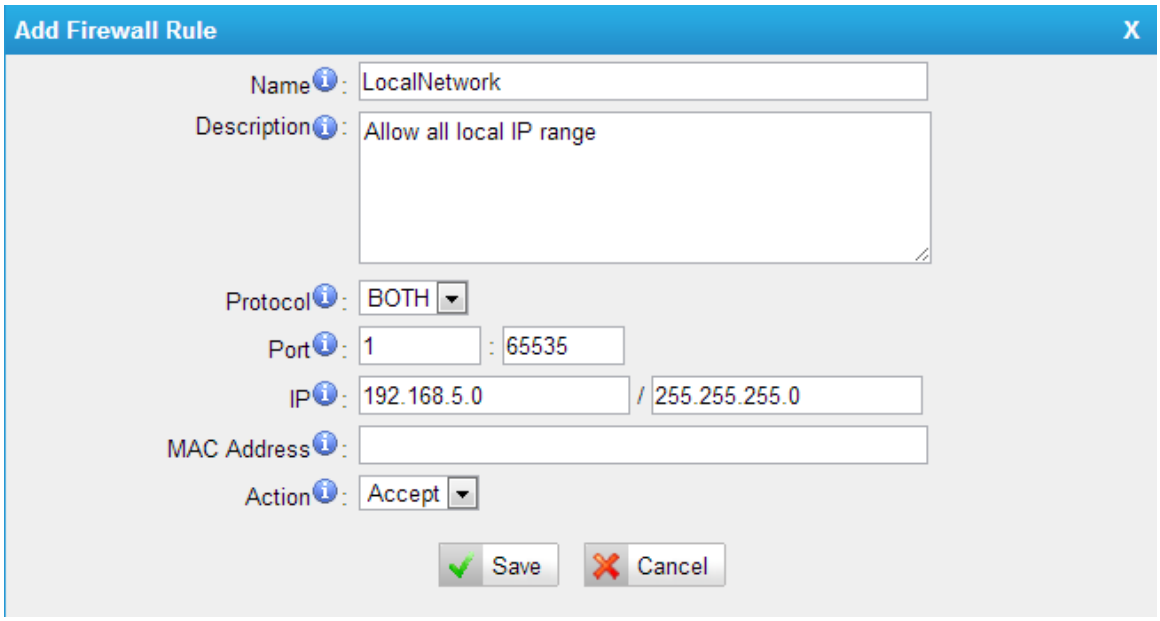


Figure 2-2

Step3. Add common rules to allow remote administrators, extensions or devices.

For example the public IP is 110.30.25.152; we can allow all ports for this trusted IP.

Name: Remote
Protocol: BOTH
Port: 1:65535
IP: 110.30.25.152/255.255.255.255
Action: Accept

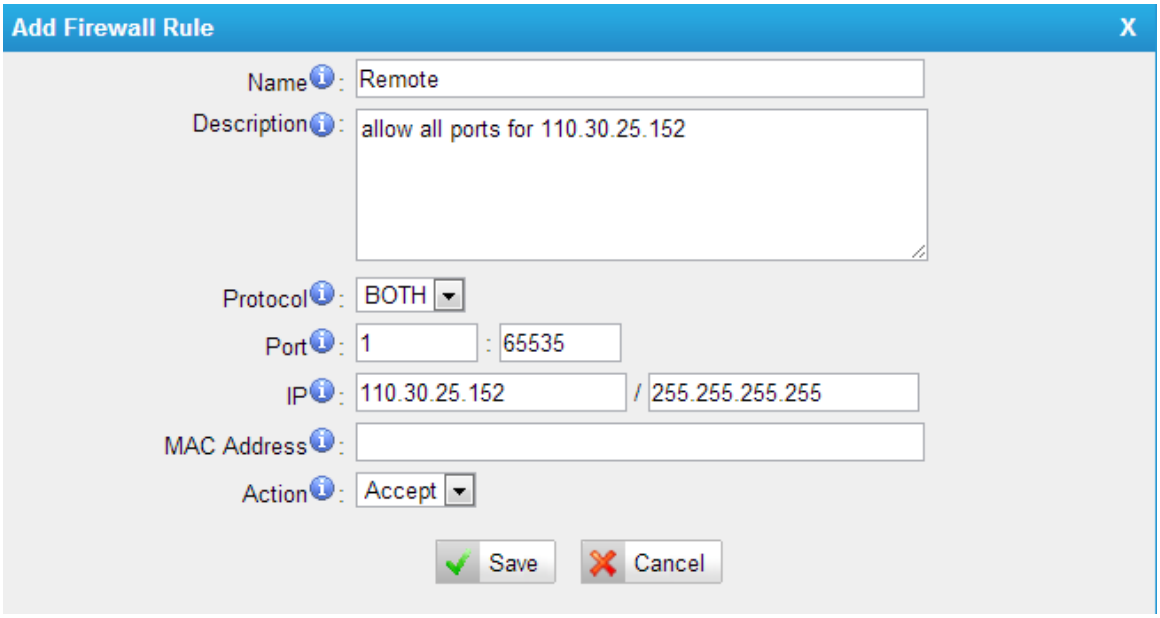


Figure 2-3

Note: Static public IP range needs to be configured here, if it's dynamic IP address that doesn't belong to a range, there is no need to configure it, but the "Drop All" in the next step should not be ticked. The IP blacklist rules will help to protect MyPBX. We recommend getting public static IP for security purpose.

Step4. Add common rules to accept the static public IP range of VoIP provider.

The ports used to contact the SIP provider is 5060 and 10000-12000 by default, if you have changed this port range, you can input it here by yourself.

For example, the IP address is 110.111.132.6, the configurations should be two parts, one is for 5060, and the second is for RTP port: 10000-12000.

Allow registry port: 5060.

Name: SIP
Protocol: UDP
Port: 5060:5060
IP: 110.111.132.6/255.255.255.255
Action: Accept

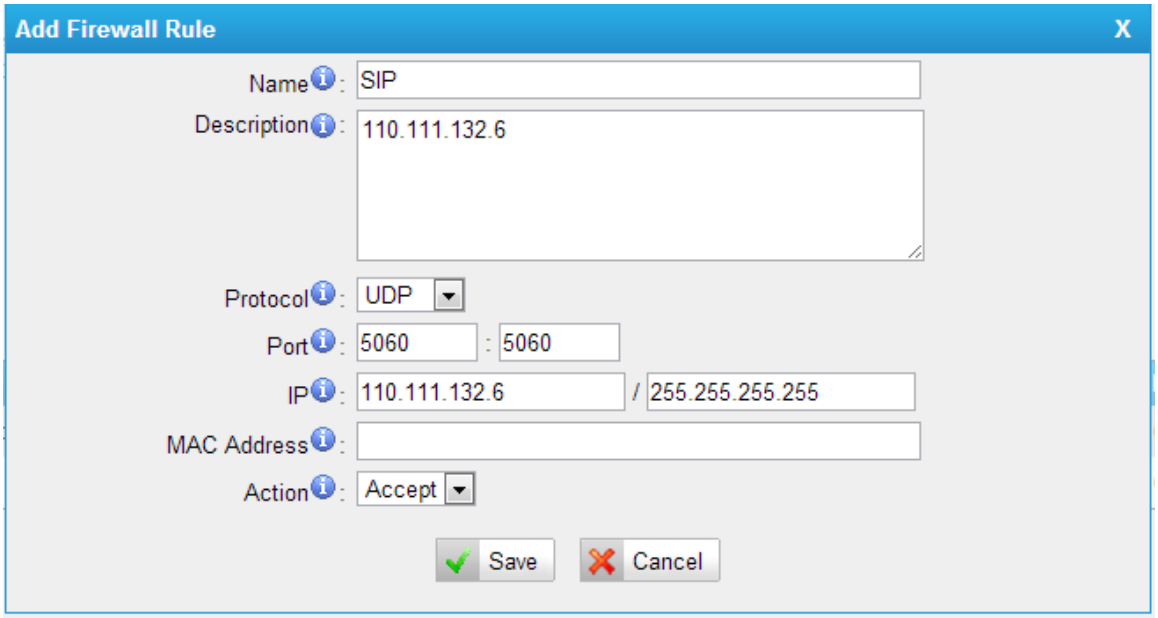


Figure 2-4

Allow RTP port range:
Name: RTP
Protocol: UDP
Port: 10000:12000
IP: 110.111.132.6/255.255.255.255
Action: Accept

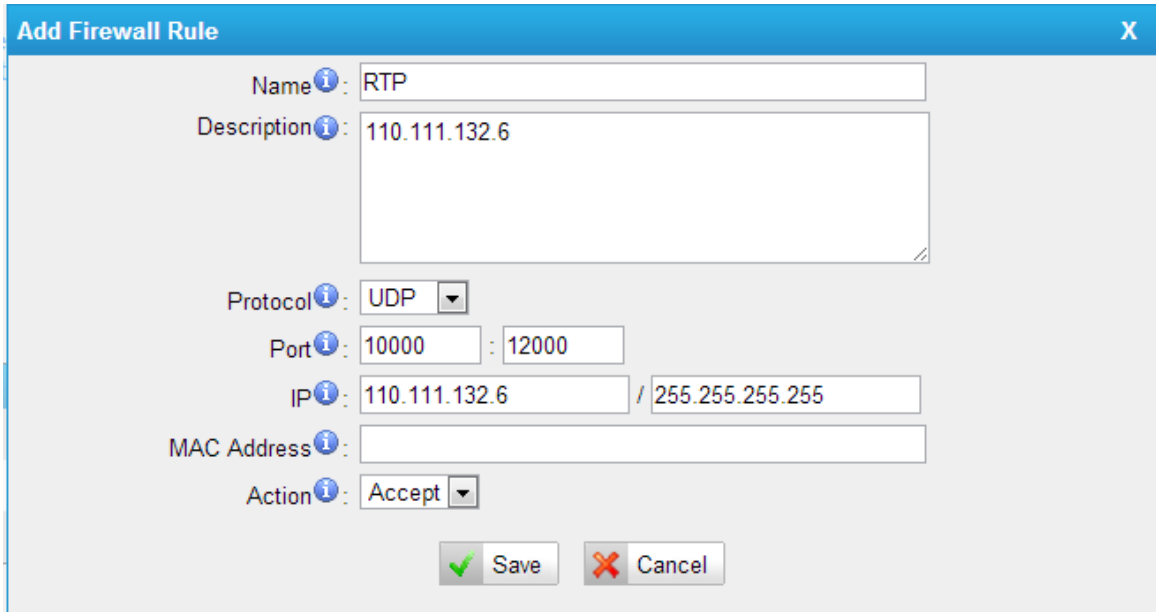


Figure 2-5

Note: If the media server of SIP provider is dynamic, and we cannot collect the IP range. We can allow the RTP range for the whole IP addresss like this:

Name: RTP_ALL
Protocol: UDP
Port: 10000:12000
IP: 0.0.0.0/0.0.0.0
Action: Accept

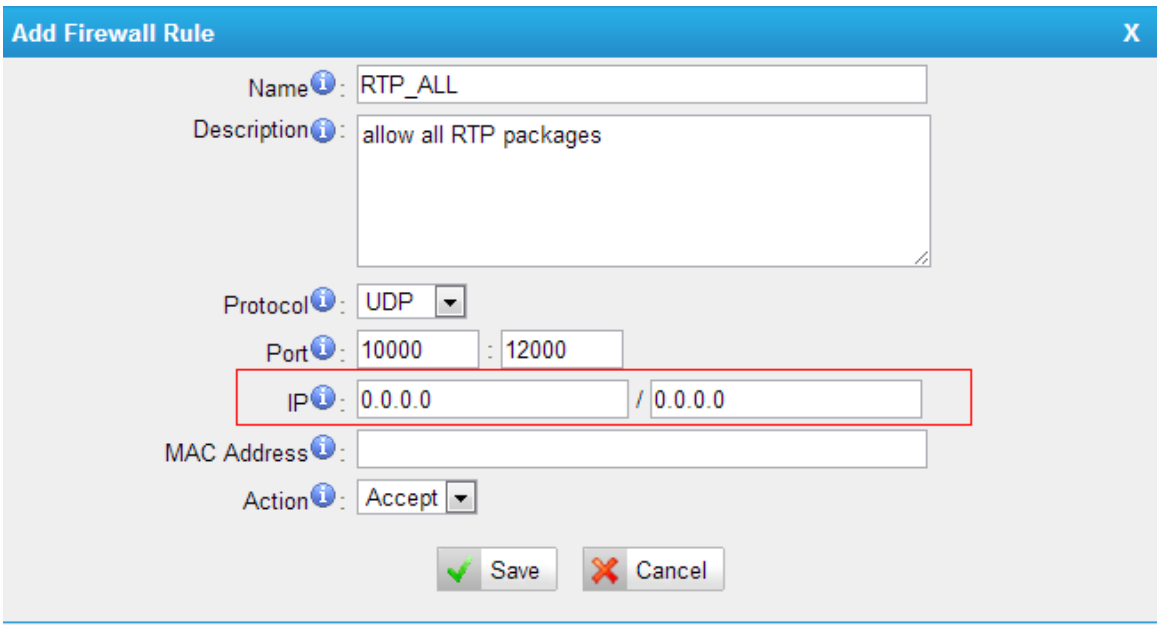


Figure 2-6

In this case, MyPBX can get rid of one-way volume issue.

Step5. Block the web connection of the other IP address that are not added into accept list.

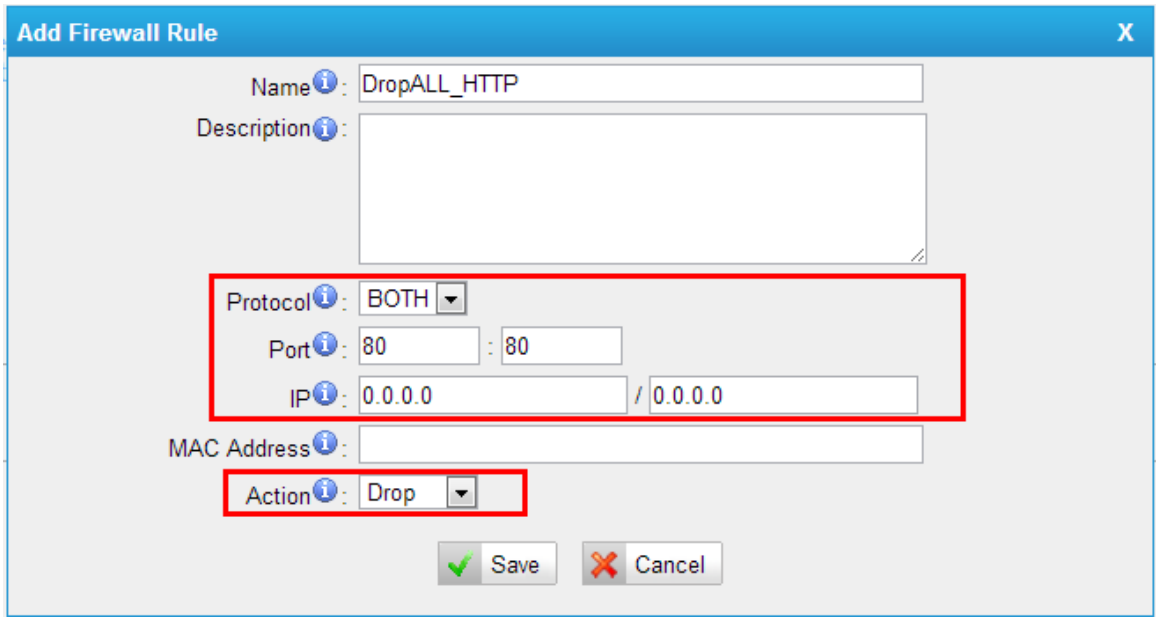


Figure 2-7

Note: Many attacks are caused by the web access, it's highly recommend to drop the untrusted connection via web interface.

Step6. Add common rules to accept the static public IP range of NTP, SMTP, and POP server.

We recommend opening all ports for NTP, SMTP, and POP server in MyPBX's firewall, and the IP address should be a static one or it belongs to a range. If it's Dyndns, there is no need to configure this rule, but the IP blacklist should be kept, and "Drop All" should not be ticked.

For example, the SMTP server is 110.30.1.123.

Name: Allow_SMTP
Protocol: BOTH
Port: 1:65535
IP: 110.30.1.123/255.255.255.255
Action: Accept

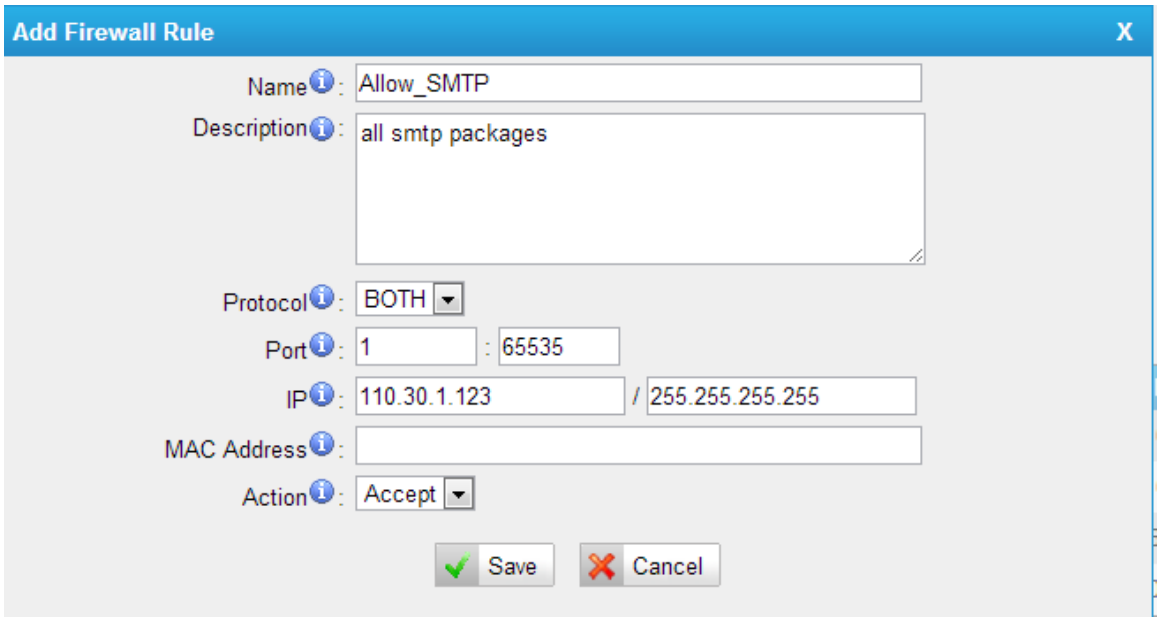


Figure 2-8

As for the rule of NTP and POP server, you can create it one by one.

Step6. Configure auto blacklist rules

Auto blacklist rules: the Server would add the IP address to the blacklist automatically if the number of the packets it sends exceeds the rule you configured.

Note: These 3 rules are created by MyPBX by default.

1) Add two auto blacklist rules for port: 5060.

Rule No.1:

Port: 5060
Protocol: UDP
IP Packets: 120
Time Interval: 60 seconds

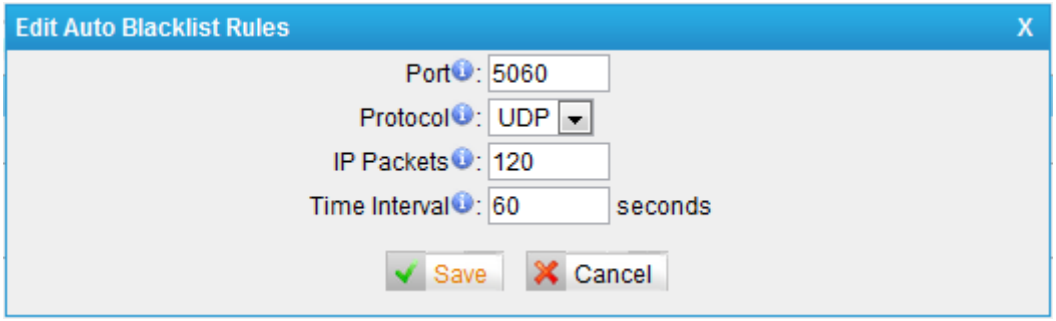


Figure 2-9

Rule No.2:

Port: 5060
Protocol: UDP
IP Packets: 40
Time Interval: 2 seconds

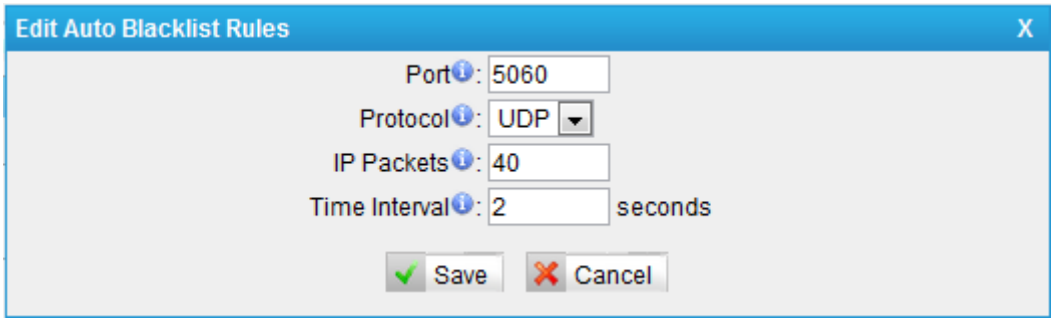


Figure 2-10

2) Add an auto blacklist rule for Port:8022

Rule No.3

Port: 8022

Protocol: TCP

IP Packets: 5

Time Interval: 60 seconds

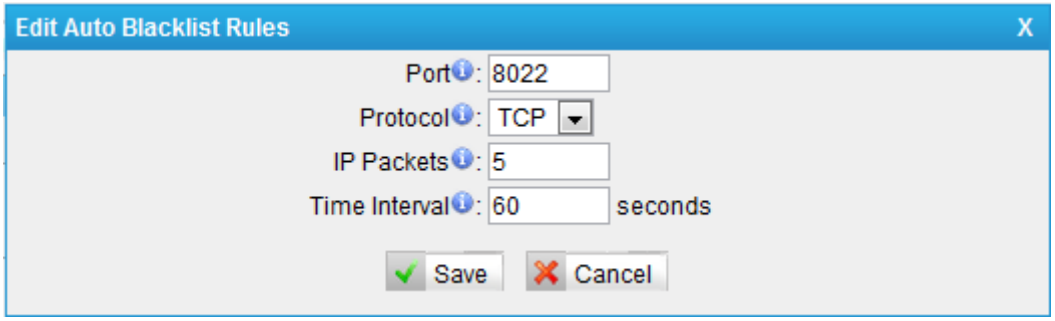


Figure 2-11

Step 7. Enable "Drop all" (If this feature is enabled, all the packets and connection that do not match the rules would be dropped.)

Warning: Before enabling this feature, please create a rule to accept the local network access, or the server might not be accessed.

Figure 2-12

Note:

1. After enabling "Drop All", the rules of auto defense and IP blacklist will not take effect. It means except the IPs and packets which are defined in the accept rules, the other connection or packets will be dropped.
2. If "Drop All" is not enabled, please don't remove the IP blacklist rules in case the system security hole exists.

Step 8. The configuration of firewall settings is completed. See the figure below.

Figure 2-13

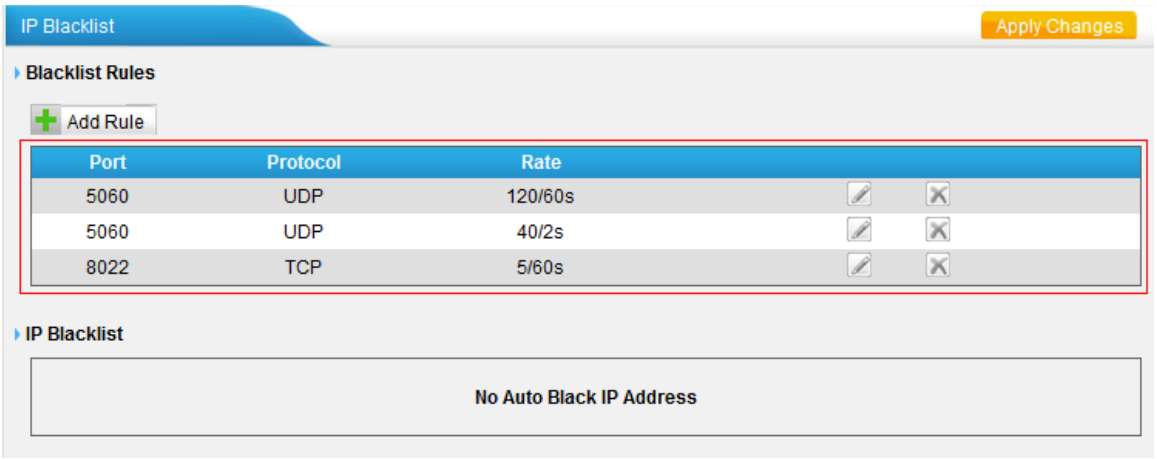


Figure 2-14

3. Service security

3.1 Disable Guest Call

3.2 Disable Guest calls

PBX→Basic Settings→SIP Settings→Advanced Settings→Allow Guest

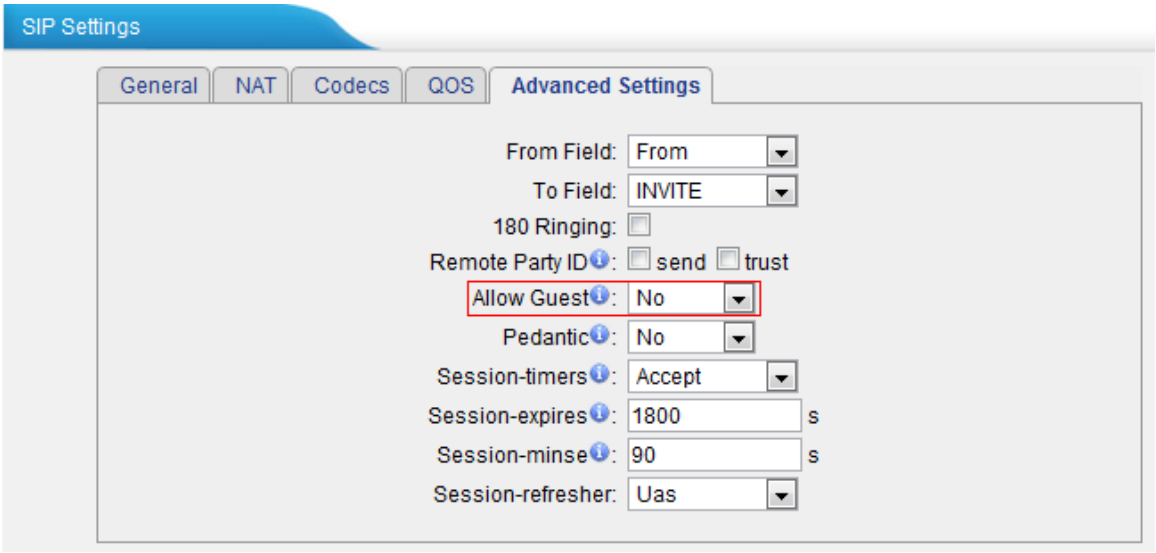


Figure 3-1

Note: Allow Guest is disabled by default; please keep it to "No" for general use.

3.2 SSH access enhancement

3.2.1 Disable SSH

Select LAN Settings→Enable SSH. If external debugging isn't required, please select "No".

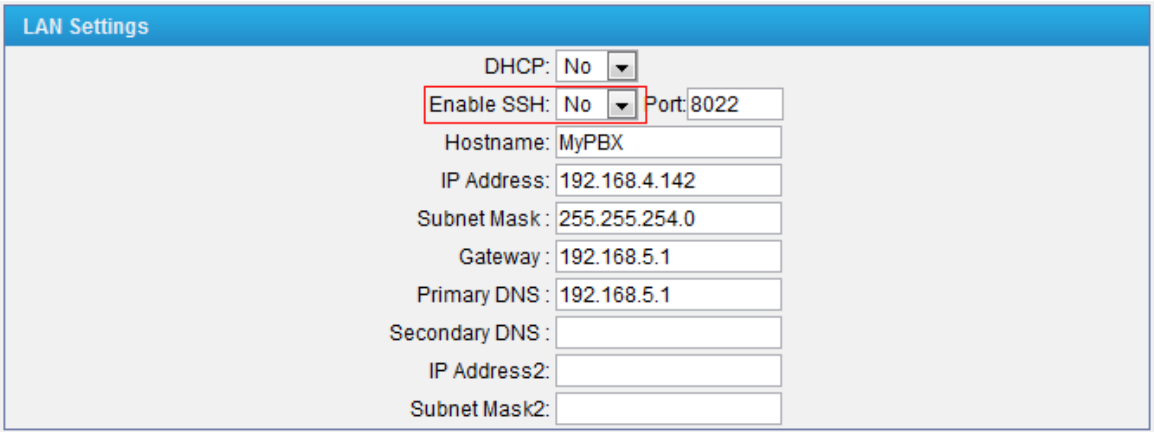


Figure 3-2

Note: SSH access is disabled by default; please keep it to "No" if not needed.

3.2.2 Change the default password for SSH

We can use the Linux command passwd to change the root password of MyPBX.

1. Log in via putty.exe.

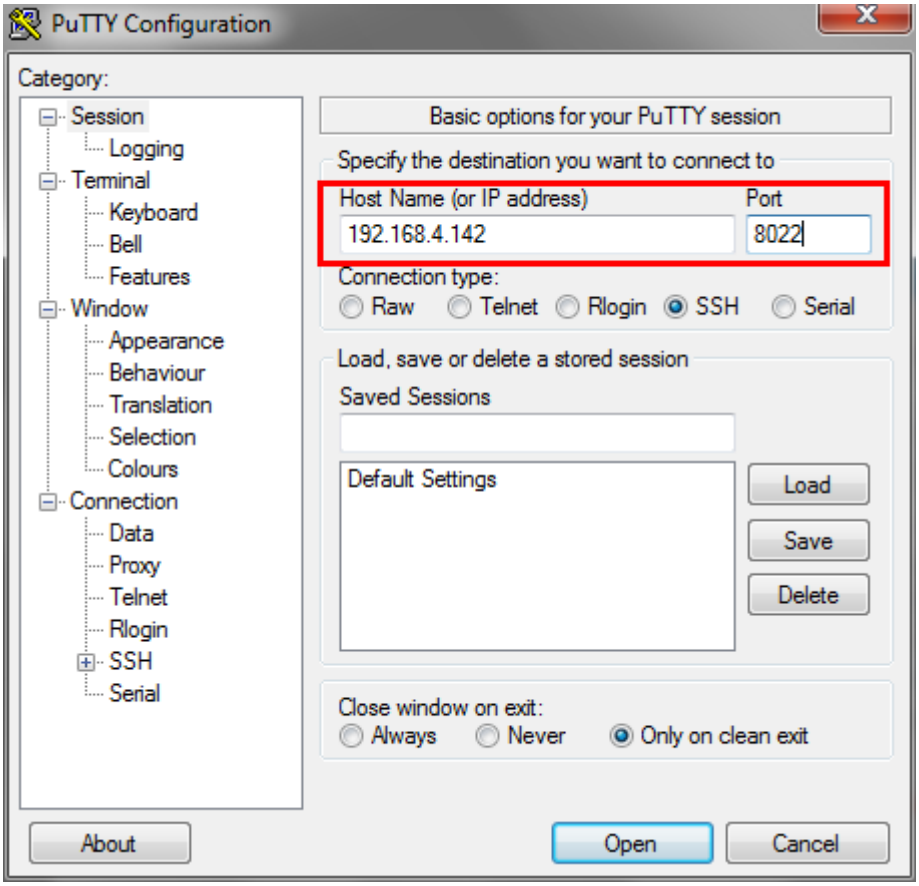


Figure 3-3

2. The default username is root and the default password is ys123456.

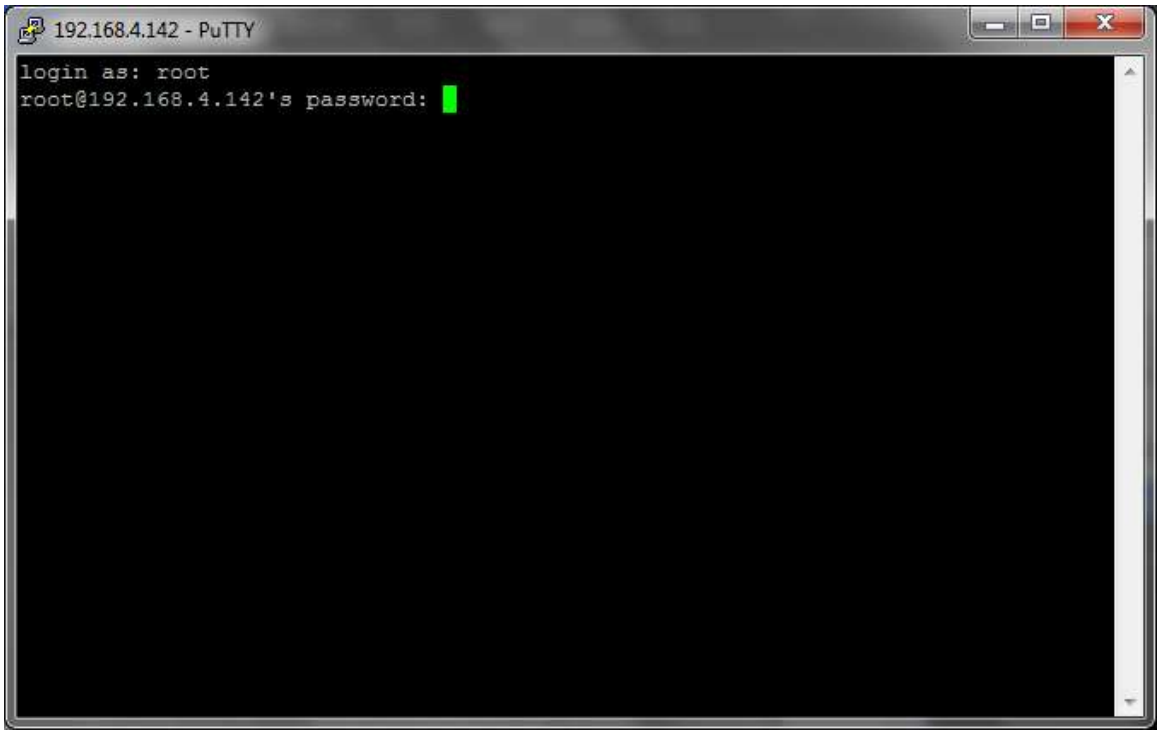


Figure 3-4

3. Use command passwd to change the root's password

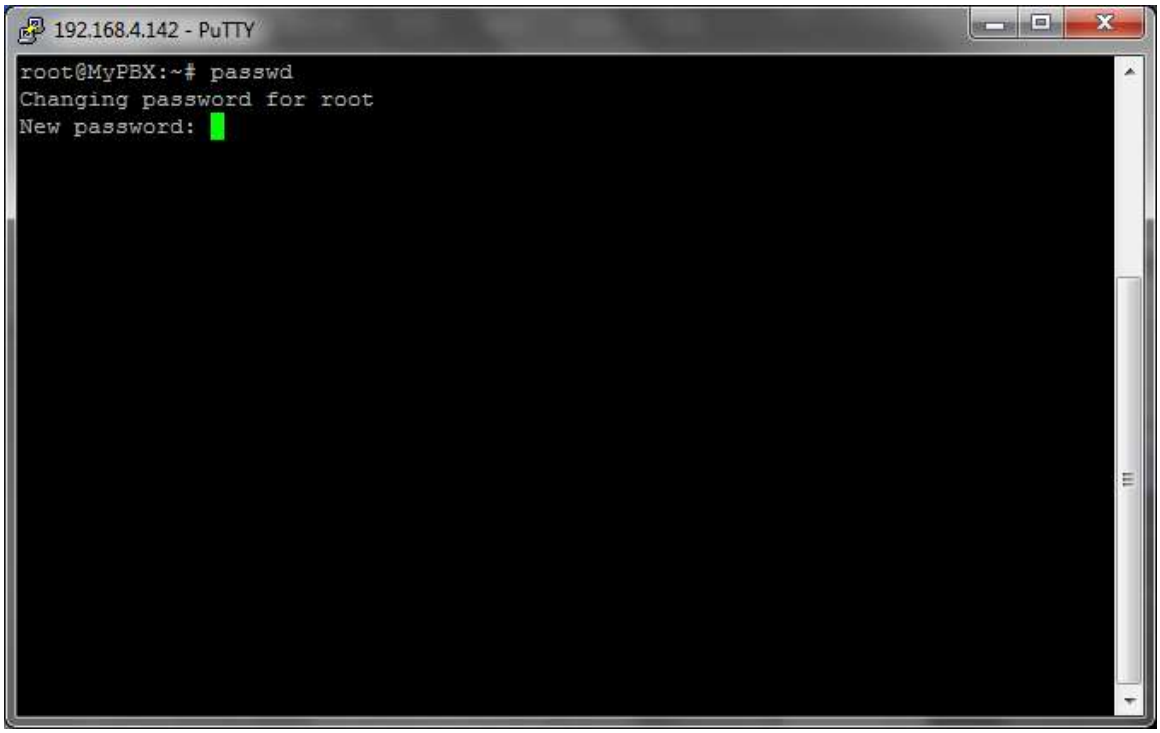


Figure 3-5

You need to input the new password twice to take effect.

3.3 AMI settings*

The Asterisk Manager Interface (AMI) allows a client program to connect to an Asterisk instance and issue commands or read events over a TCP/IP stream. Integrators will find this particularly useful when trying to track the state of a telephony client inside Asterisk, and directing that client based on custom (and possibly dynamic) rules.
For more information, you can refer to this page:
http://www.voip-info.org/wiki/view/Asterisk+manager+API

Note: this feature is disabled by default; there is no need to enable it for general use. If it's enabled, please change account and configure IP restriction.

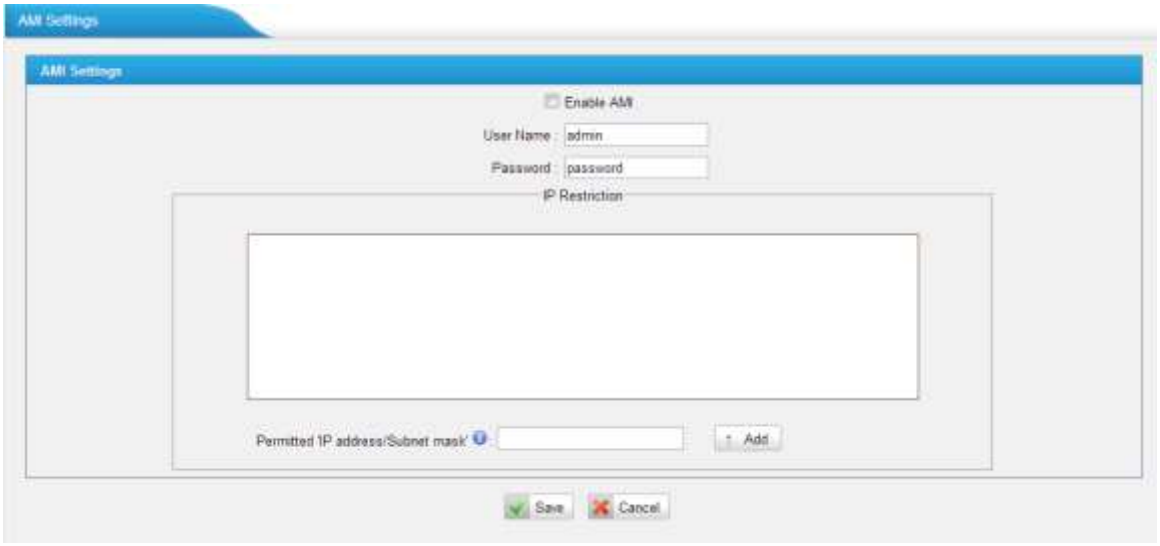


Figure 3-6

To manage the accounts to access AMI, we can configure it in AMI page directly. Click System→System Preferences→AMI Settings.

For example, the AMI account I want is:
User name: Developer
Password: Developer
The only IP address that's allowed to log in is 192.168.1.71.

We can configure it like this:

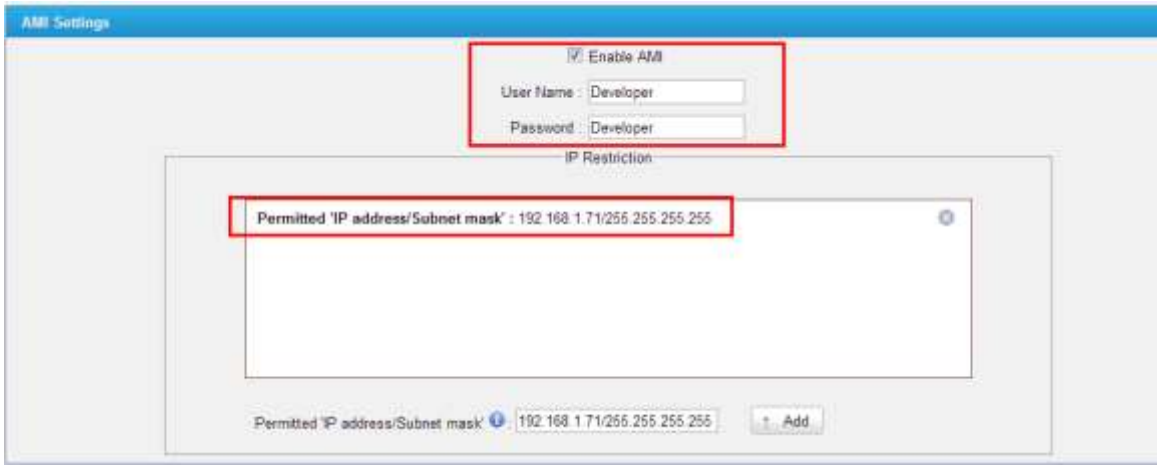


Figure 3-7

Save it and apply the changes.
To confirm more details, please try command "cat /etc/asterisk/manager.conf"

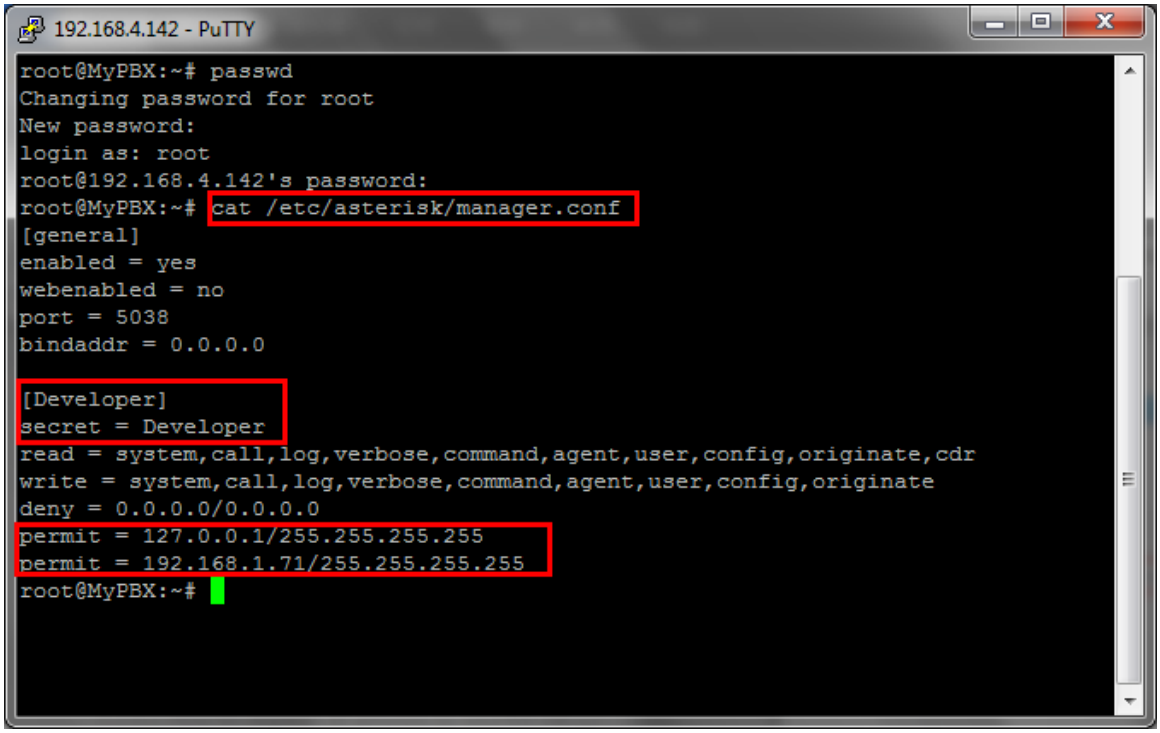


Figure 3-8

3.4 TFTP*

MyPBX can work as a TFTP server when using "phone provisioning", and this feature is enabled by default. If all the phones are well provisioned, you can disable this access to protect the configuration files of MyPBX.

Click "System→Security Center→Service" to disable it directly.

Figure 3-9

3.5 Database Grant*

MyPBX has integrated MySQL since x.18.0.xx, which provides convenience for users to manage the CDR and the Recording log. To protect the database access, we need to set up user name and password separately before login.

There is no account configured by default, if you need to connect the database using third party software, you need to set up this first.

For example, username: Harry, password: Harry123

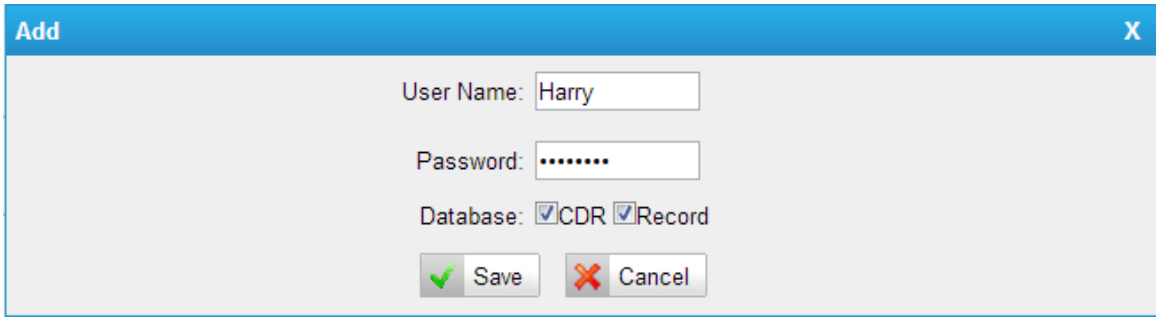


Figure 3-10

Save it and apply the changes.

Figure 3-11

When logging in using other software, we can check the CDR.

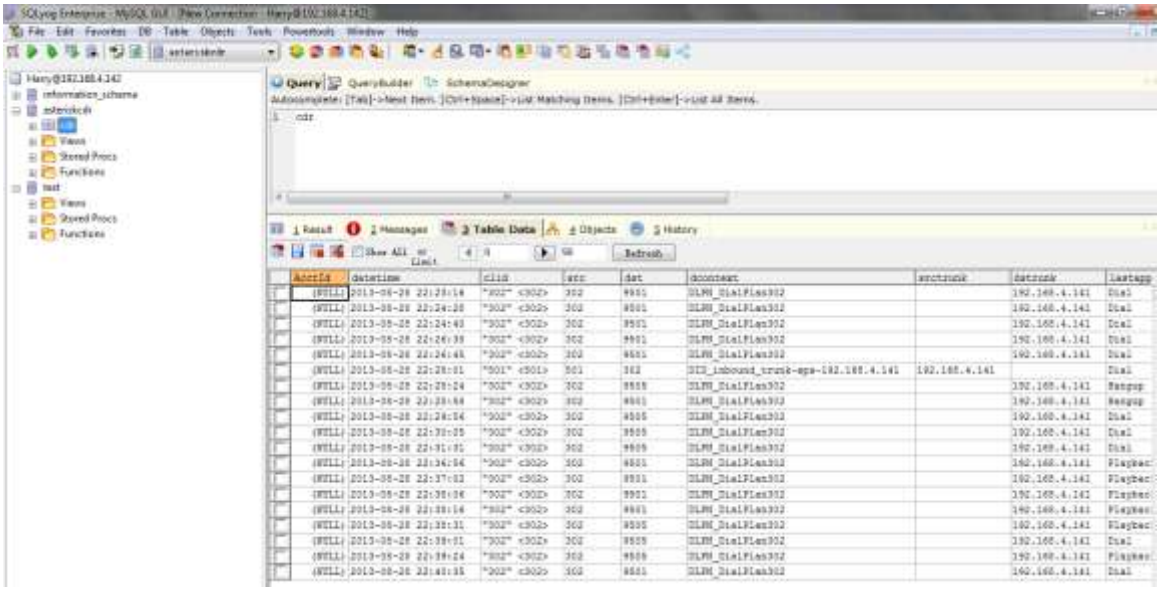


Figure 3-12

3.6 Alert settings

After enabling alert settings, if the device is attacked, the system will notify users the alert via call or e-mail. The attack modes include IP attack and Web Login.

3.6.1 IPATTACK

When the system is attacked by some IP addresses, the firewall will add the IP to auto IP Blacklist and notify the user if it match the protection rule.
Example: Configure to notify extension 500, outbound number 5503301 and E-mail alert@yeastar.com.
configuration could be as below.

Phone Notification Settings:
Phone Notification: Yes
Number: 500;5503301
Attempts: 1
Interval: 60s
Prompt: default

Note: If there's an outbound number to notify, the number should fit the dial pattern of the outbound route.

E-mail Notification Settings:
E-mail Notification: Yes
To: alert@yeastar.com
Subject: IPAttack

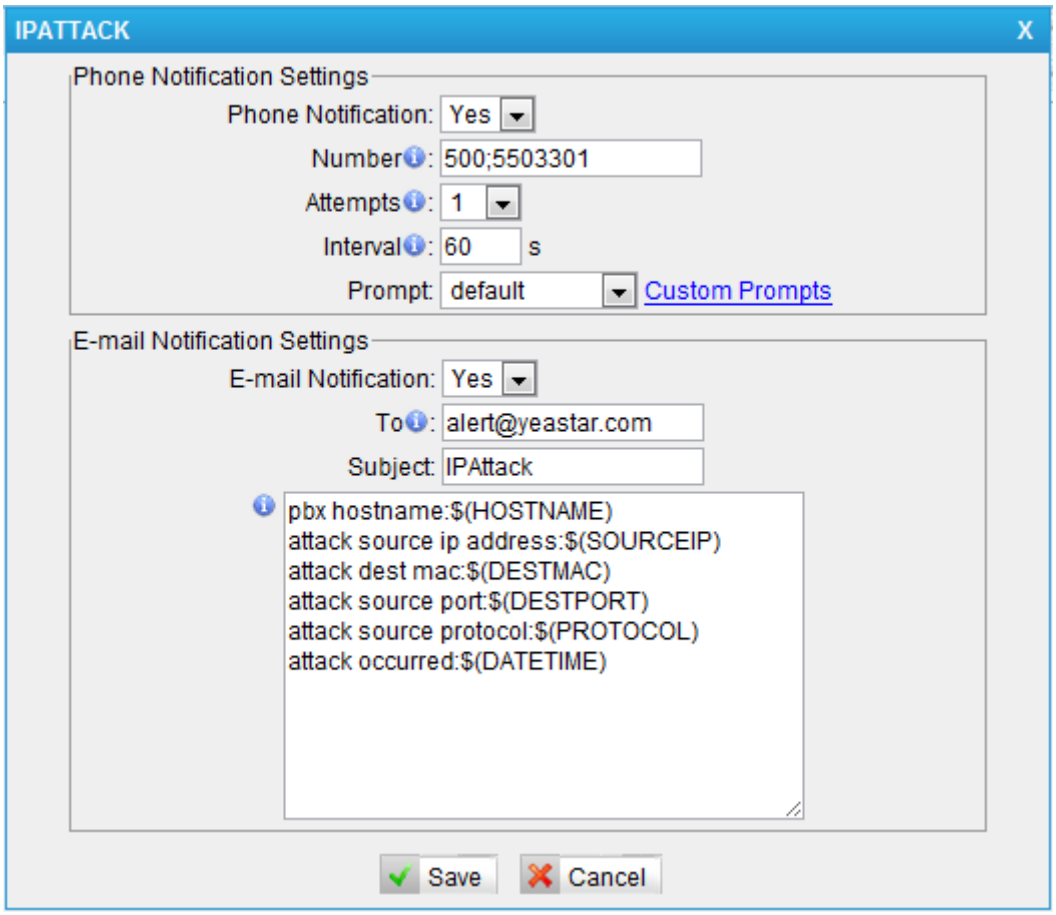


Figure 3-13

3.6.2 WEBLOGIN

Enter the password incorrectly five times when logging in MyPBX Web interface will be deemed as attack, the system will limit the IP login within 10 minutes and notify the user. Example: Configure to notify extension 500, outbound number 5503301 and E-mail alert@yeastar.com.
configuration could be as below.

Phone Notification Settings:

Phone Notification: Yes
Number: 500;5503301
Attempts: 1
Interval: 60s
Prompt: default

Note: If there's an outbound number to notify, the number should fit the dial pattern of the outbound route.

E-mail Notification Settings:

E-mail Notification: Yes
To: alert@yeastar.com
Subject: WebLogin

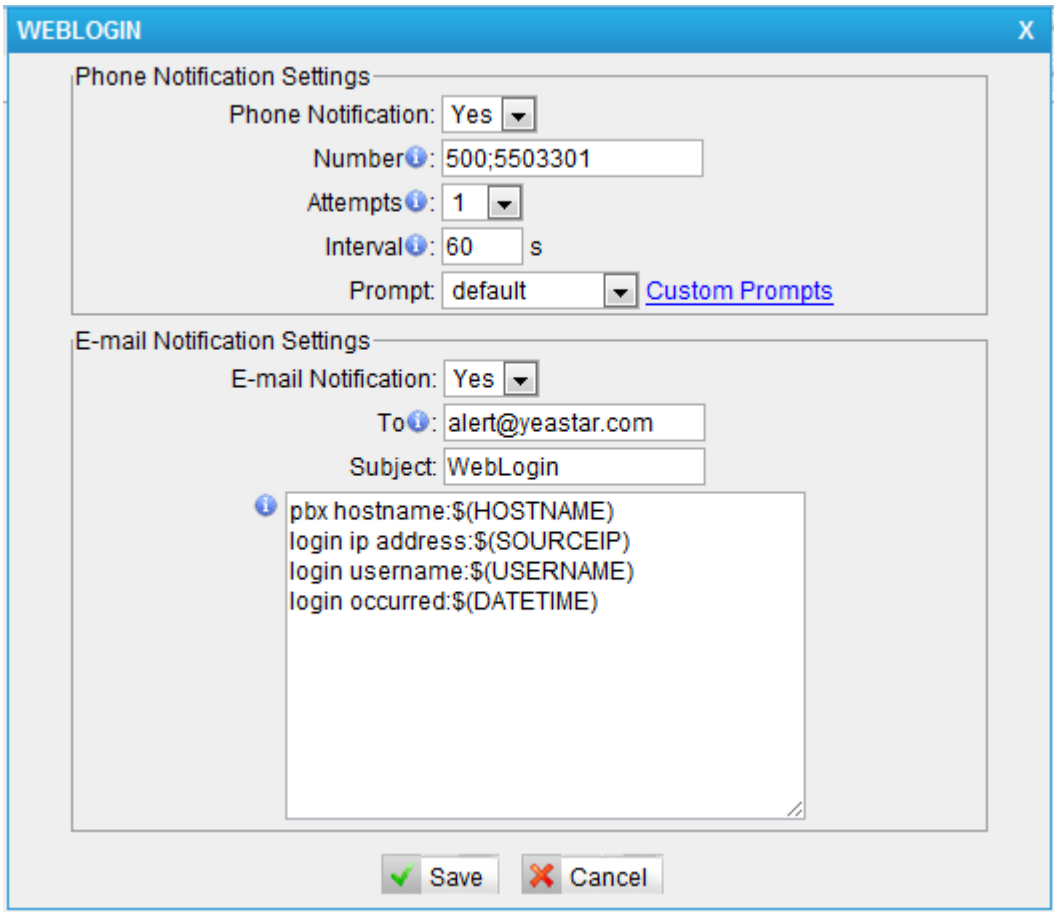


Figure 3-14

4. International call limit

4.1 Limit call credit at provider side

We can ask VoIP/PSTN/ISDN provider for help to limit the credit of international calls in advance, then the hacker cannot dial international calls. Each provider has its own policy. You can also ask provider to disable international call if not needed.

4.2 Set password for international call

MyPBX allows you to configure password for outbound routes. Click "PBX→Outbound Call Control→ Outbound Route".

For example, the password you need is 5503333
Dial pattern: 00. <Don't miss the dot here>
Password: 5503333
Choose the allowed extension and the trunk to the right side like this:

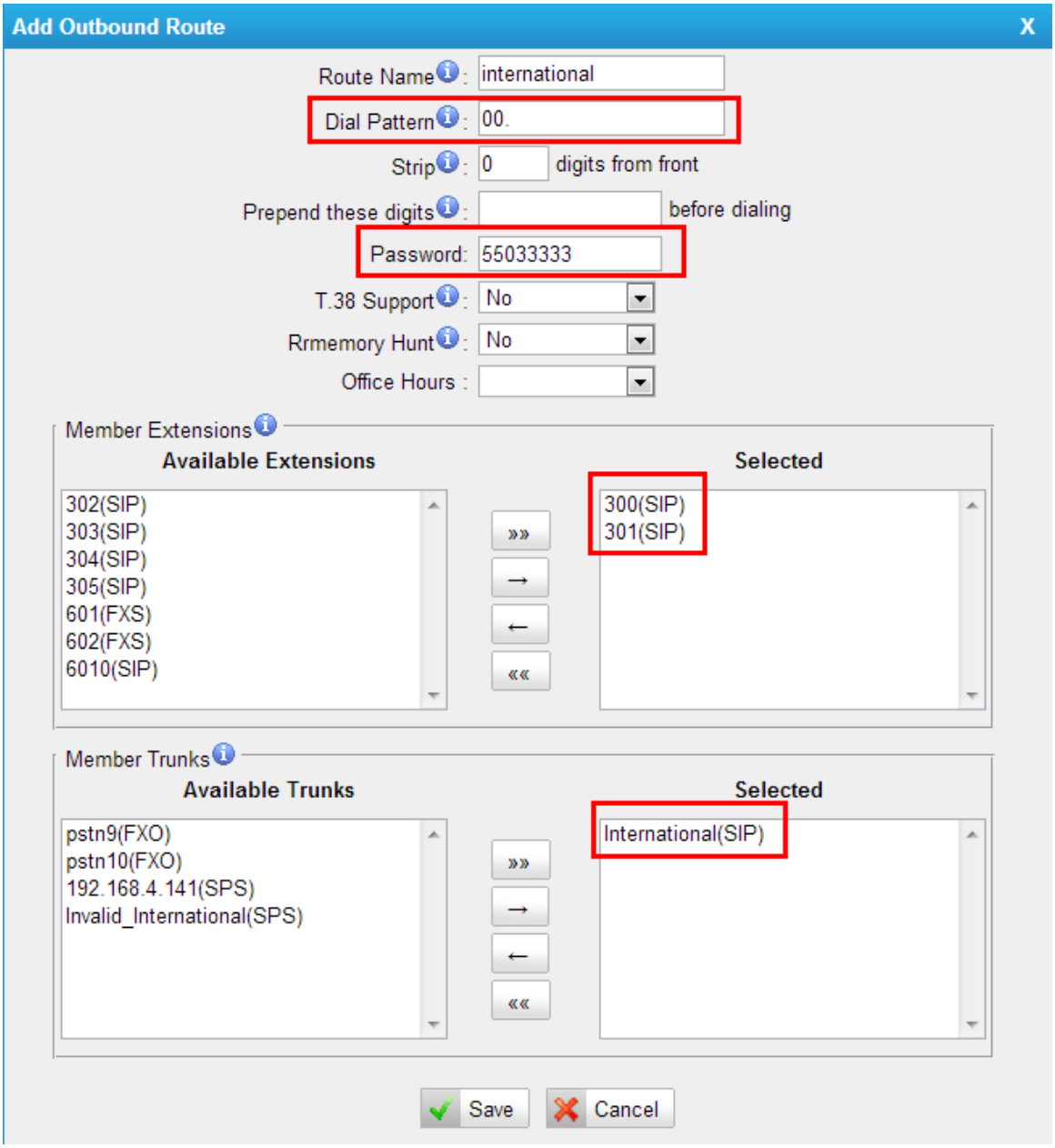


Figure 4-1

Save and apply the changes, when 300 and 301 pick up headsets and dial a international number, MyPBX will ask for the password, if passed, the call will be dialed out. If not, the call will be dropped.

4.3 Disable international call in MyPBX

We can ask the provider for help to disable international calls in advance, if it's not possible, we can configure the rules in MyPBX side to drop all the international calls. Here are the detailed steps.

Step1. Create an invalid SIP trunk

Create an invalid SIP trunk in "PBX→VoIP trunk→Service Provider". The IP address can be an invalid one, like 127.0.0.1

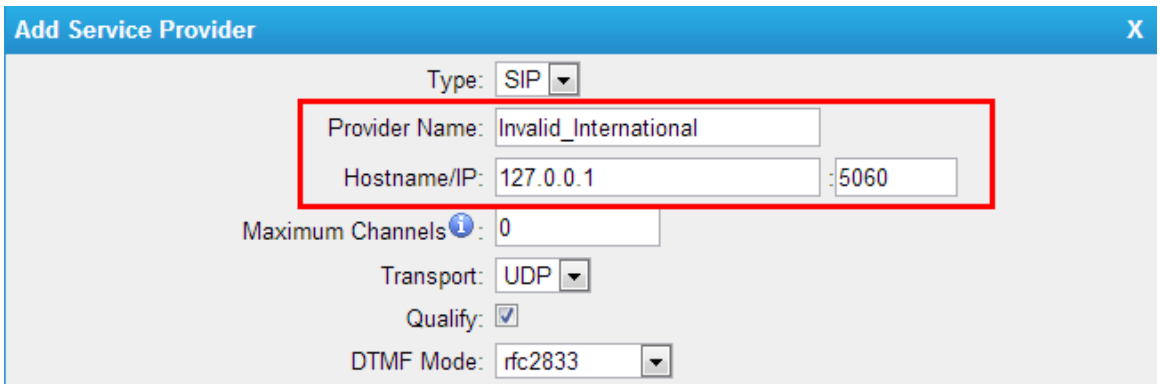


Figure 4-2

Save it and apply the changes. The status of this trunk is unreachable of course. That's what we want.

Step2. Create an oubount route for all extensions and this trunk to route international calls.

ClicK "PBX→Outbound Call Control→Outbound Route", create a new one:
Name: NoInternational
Dial pattern: 00. <Don't miss that dot here>
Strip: 0
Choose all extensions and that special trunk (Invalid_international) to the right side.

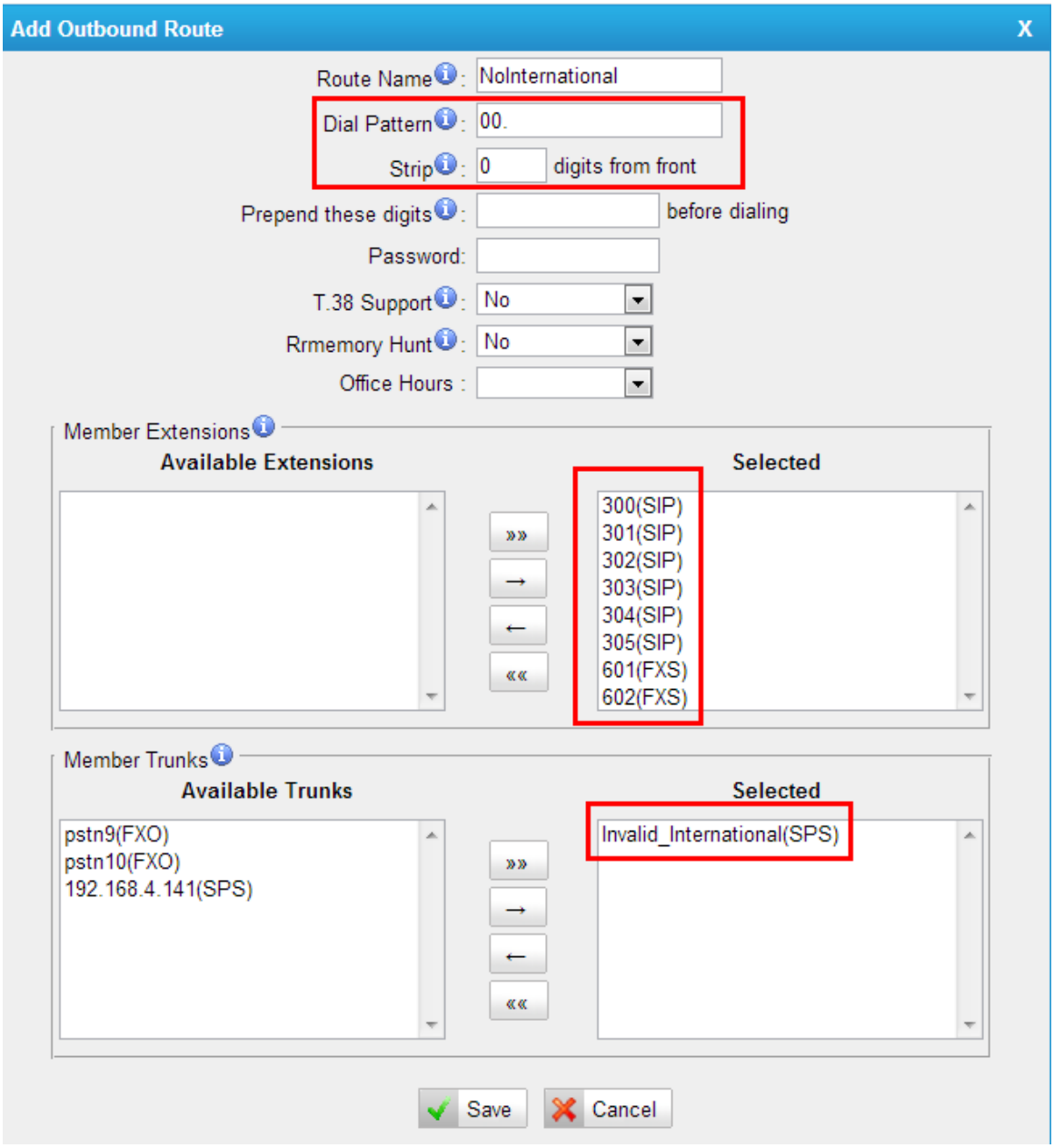


Figure 4-3

Save it and apply the changes. Then click the arrow at the left side to set it to the top.

Figure 4-4

In this case, all international call requests will be routed to this invalid trunk. Ie. The call is dropped directly.

Appendix I. How to use TLS in MyPBX.

I.1 How to register IP phones to MyPBX via TLS

MyPBX is working as a SIP server, IP phones register to MyPBX as extensions via TLS.

1. Enable TLS in MyPBX's web interface

Click "PBX→SIP settings→General" to get the settings about TLS, which is disabled by default. If you are using MyPBX standard, please find it in "Internal Settings→SIP Settings" page.

Figure I-1

·TLS Port
Port use for Sip registrations, Default is 5061.

·TLS Verify Server
When using MyPBX as a TLS client, whether or not to verify server's certificate. It is "No" by default.

·TLS Verify Client
When using MyPBX as a TLS server, whether or not to verify client's certificate. It is "No" by default.

·TLS Ignore Common Name
Set this parameter as "No", then common name must be the same with IP or domain name.

·TLS Client Method
When using MyPBX as a TLS client, specify the protocol for outbound TLS connections. You can select it as tlsv1, sslv2 or sslv3.

Figure I-2

Note:

1. For security reason, we recommend enabling "TLS Verify Client" and disabling "TLS Ignore Common Name", in which case, MyPBX will verify IP phone's Certificate, the common name inside CA should be the same as its IP or domain name.
2. TLS Client Method: it's the TLS method of IP phone; you can contact the manufacturer of the IP phone to get that.
3. You need to reboot MyPBX to take effect after enabling TLS.

2. Prepare the whole certificates for TLS

Here are the certificates of MyPBX and IP phones for TLS registry as the screen shot above:

MyPBX's CA: CA.crt.
MyPBX's server certificate: asterisk.pem.
IP phone's CA: CA.crt or CA.csr.
IP phone's server certificate: client.pem.

The certificate is generated via the toolkit OpenSSL, you can compile the source package from http://www.openssl.org/, or download the tool used here, download link: www.yeastar.com/download/tools/TLS_CA_Tool.rar

You can find the files inside the package like these:

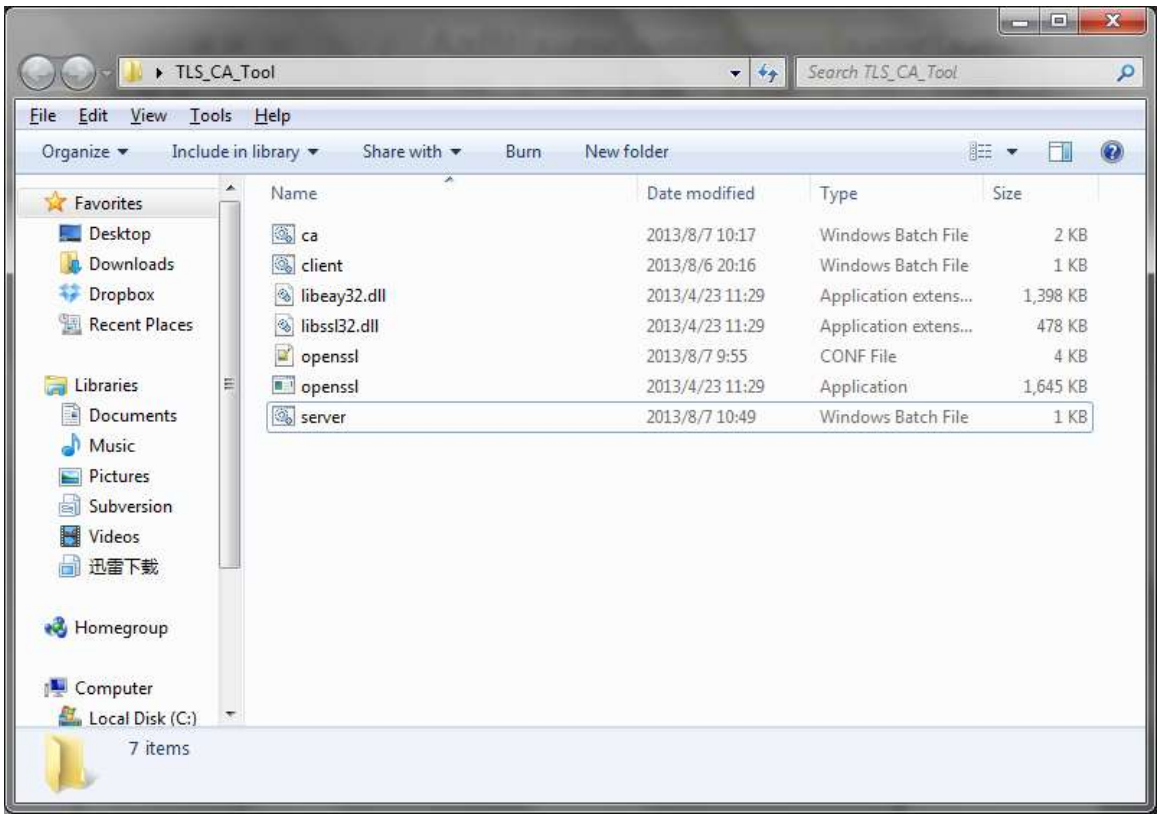


Figure I-3

Ca.bat: Make the CA.crt for IP phone and MyPBX
Client.bat: make the "client.pem", it's the "IP phone's server certificate".
Server.bat: make the "asterisk.pem", it's the "MyPBX's server certificate".

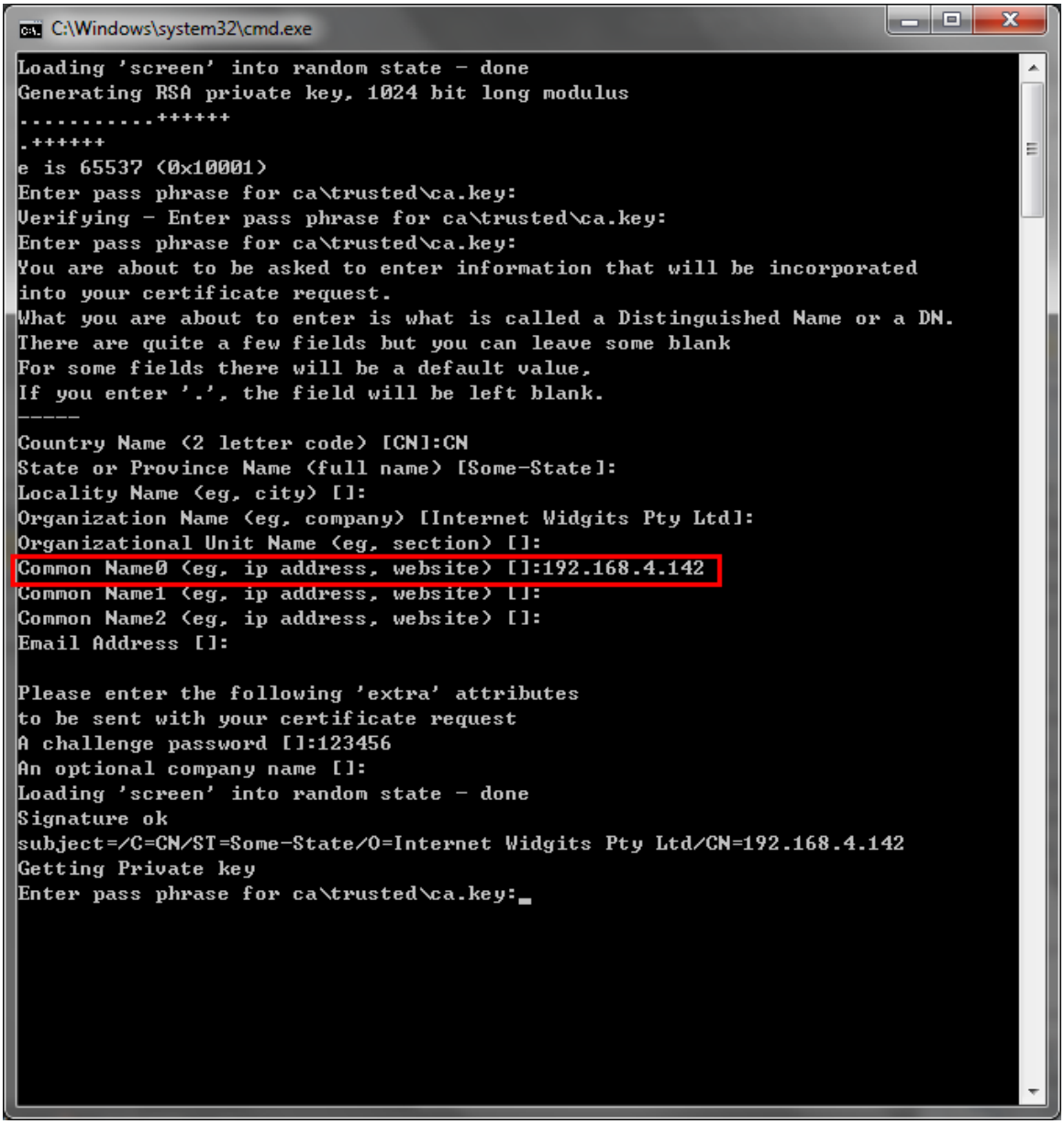
Here are the steps to make all the certificates.

Step1. Prepare MyPBX's CA: CA.crt

Double click ca.bat

Figure I-4

Just follow the guide to input the information of MyPBX step by step.
In this example, MyPBX's IP address is 192.168.4.142.


C:\Windows\system32\cmd.exe
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....++++++
.++++++
e is 65537 (0x10001)
Enter pass phrase for ca\trusted\ca.key:
Verifying - Enter pass phrase for ca\trusted\ca.key:
Enter pass phrase for ca\trusted\ca.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [CN]:CN
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name0 (eg, ip address, website) []:192.168.4.142
Common Name1 (eg, ip address, website) []:
Common Name2 (eg, ip address, website) []:
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:
Loading 'screen' into random state - done
Signature ok
subject=/C=CN/ST=Some-State/O=Internet Widgits Pty Ltd/CN=192.168.4.142
Getting Private key
Enter pass phrase for ca\trusted\ca.key:

Figure I-5

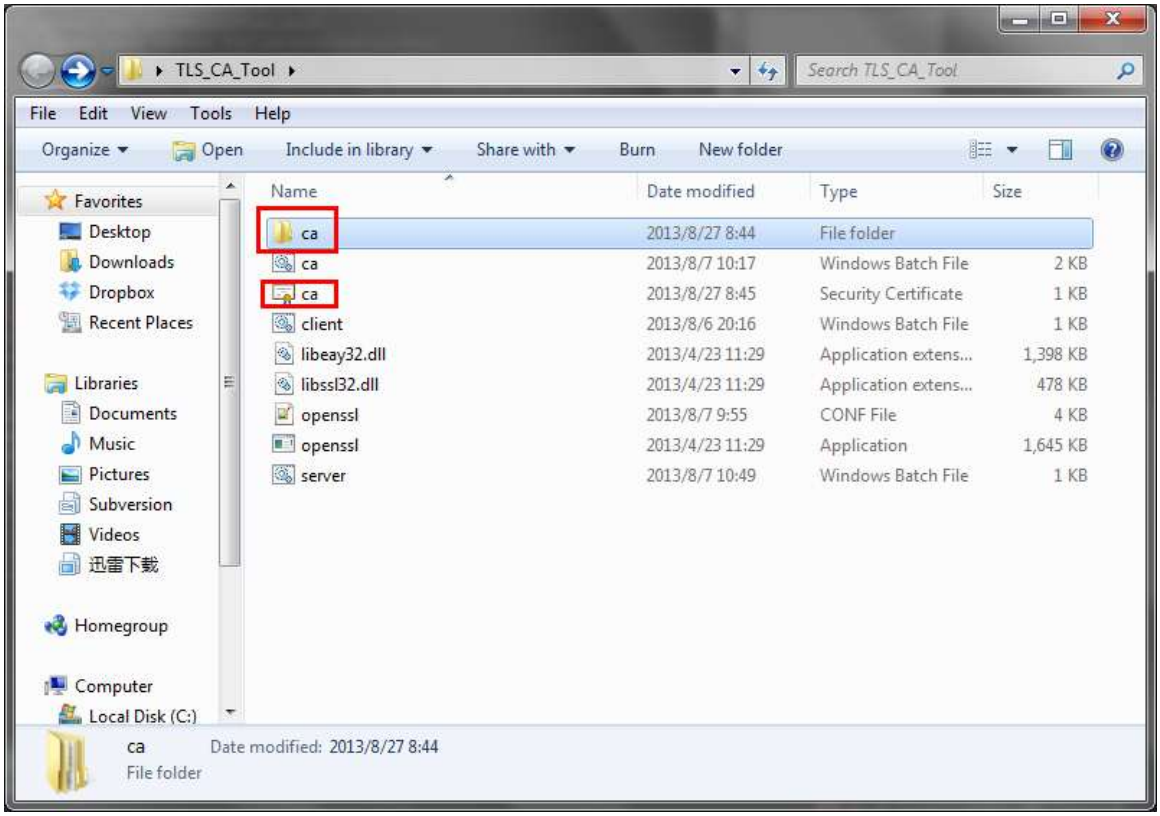


Figure I-6

This ca.crt is the same as the one in folder /TLS_CA_Tool/ca/trusted/.

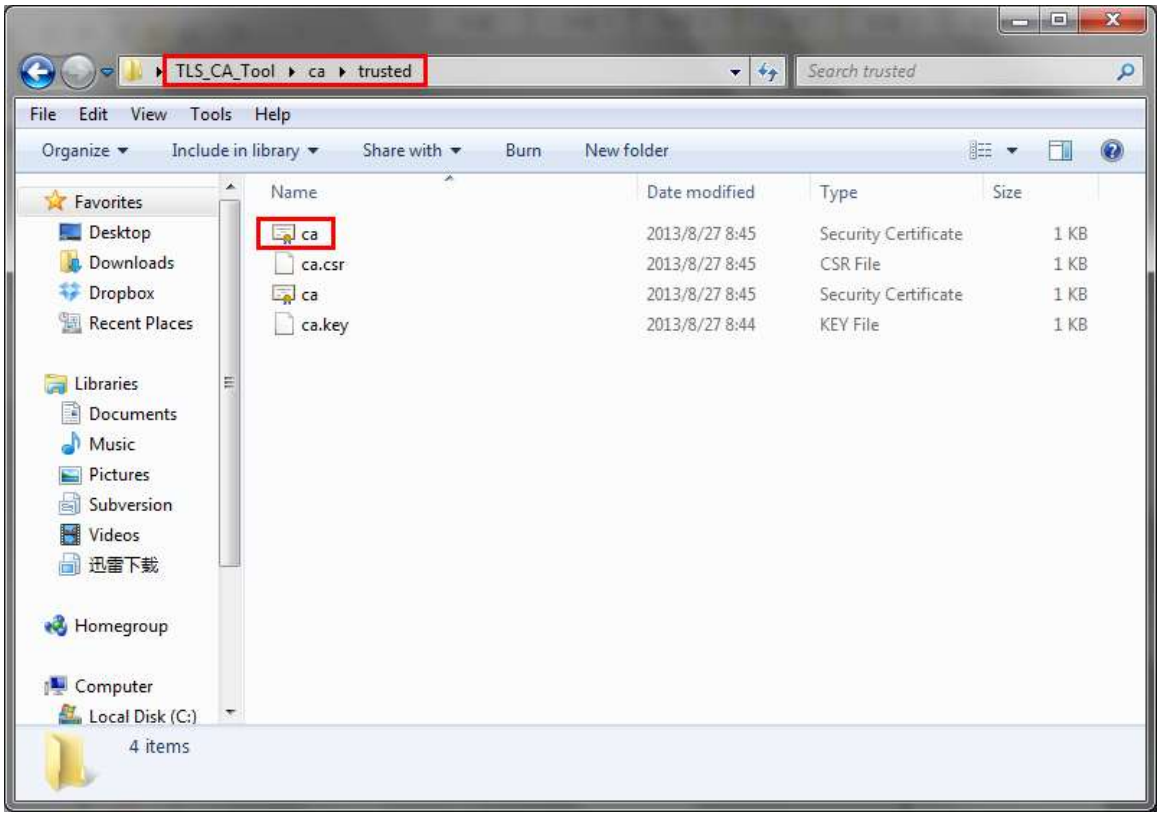


Figure I-7

MyPBX's CA: CA.crt is generated successfully.

Step2 Prepare "asterisk.pem", "MyPBX's server certificate"

We need the CA.crt and CA.key to make the server certificate.
Double click "server.bat".

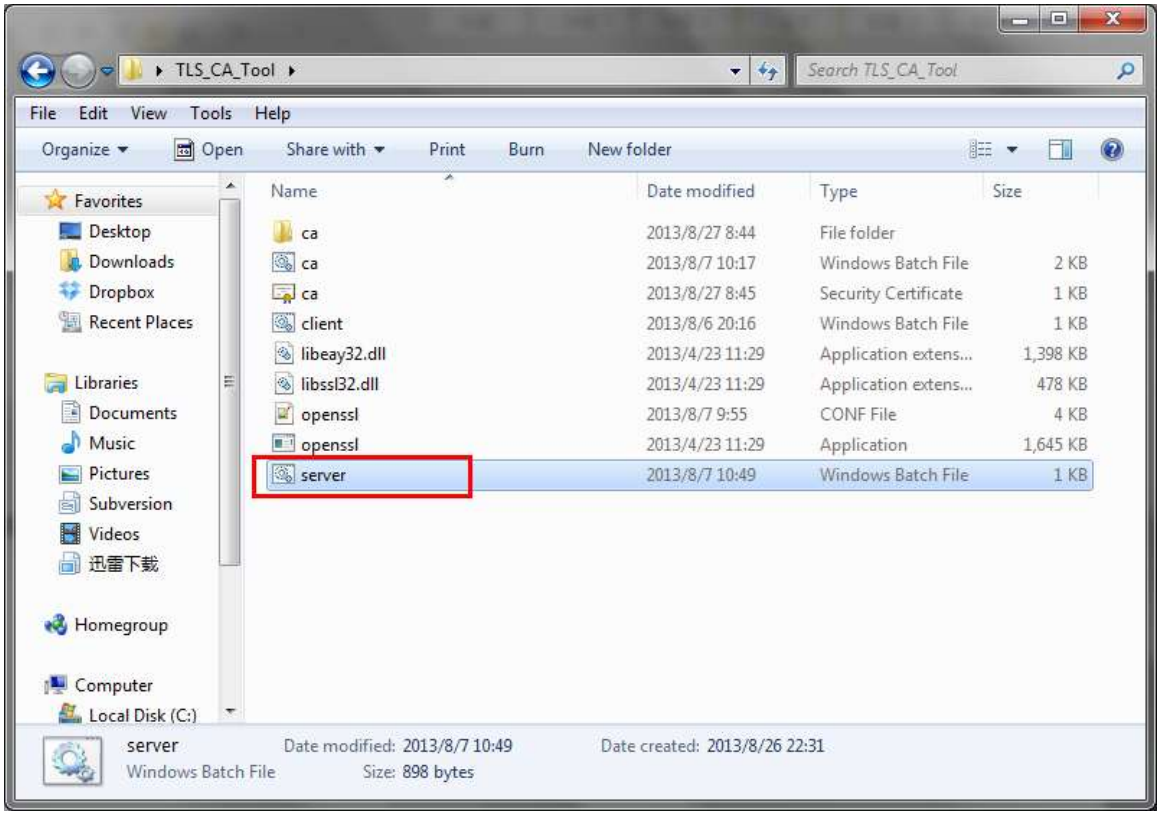


Figure I-8

Follow the guide to input information step by step, and make sure the information you have input matches the one you have input in Step1.

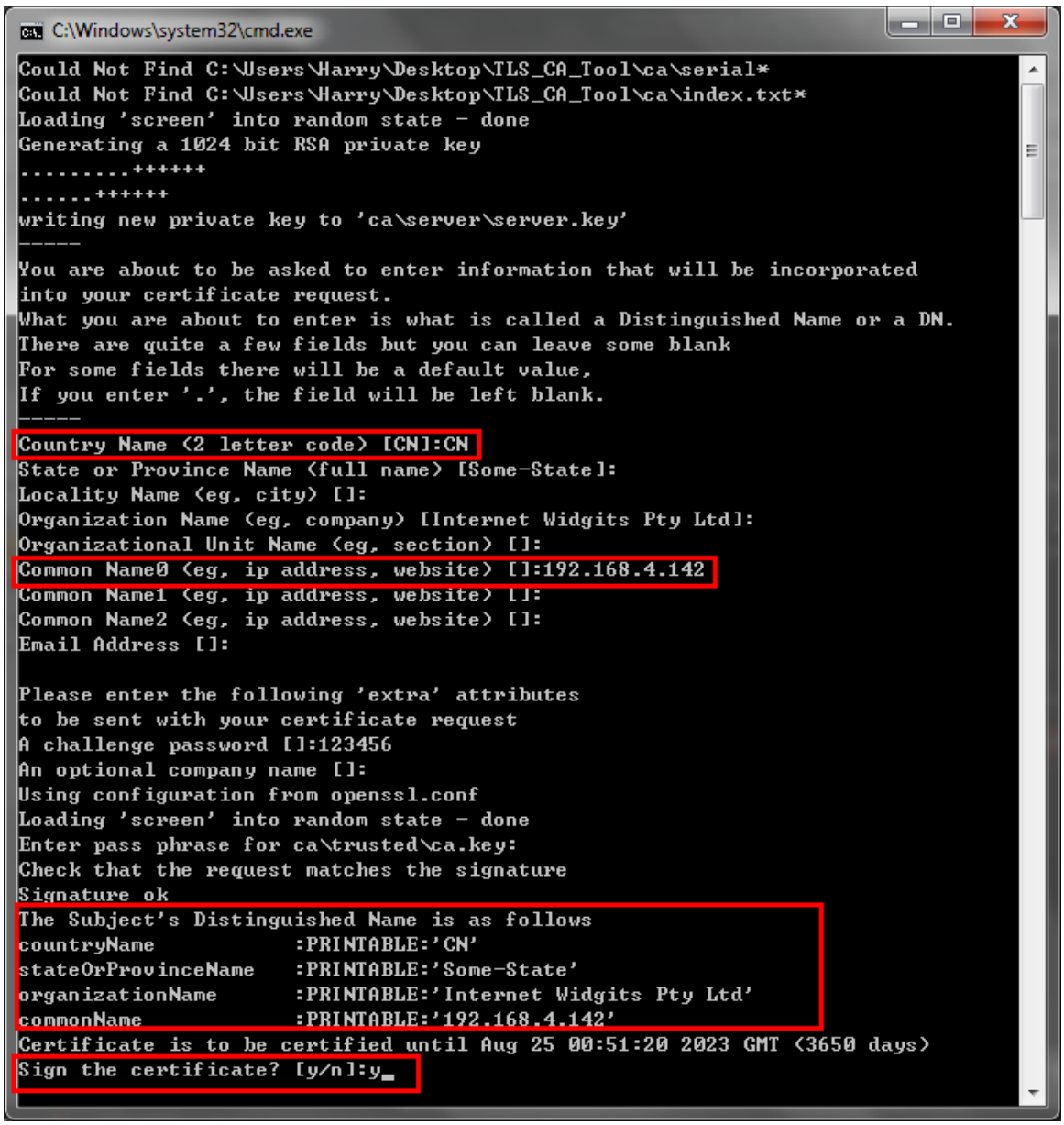


Figure I-9

Check the whole information then input "y" to continue. When done, you can find the asterisk.pem as the following picture shows.

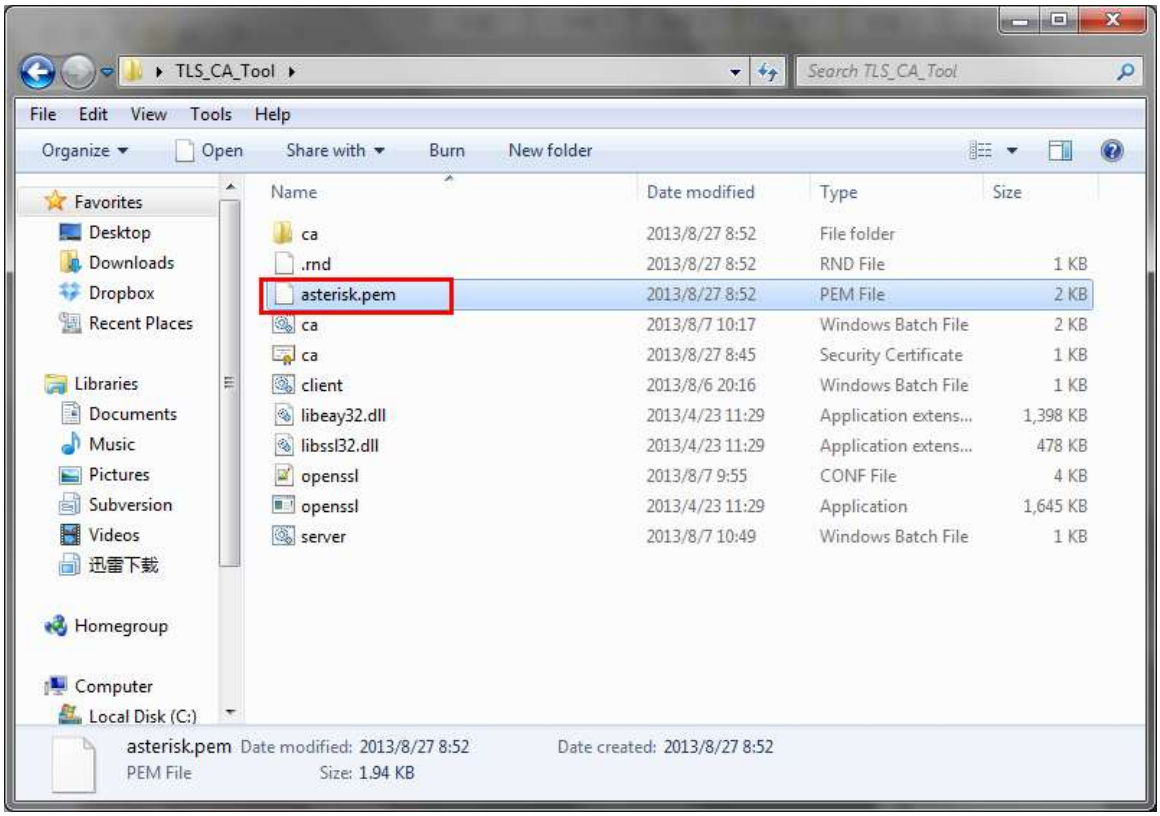


Figure I-10

asterisk.pem, the "MyPBX's server certificate" is generated successfully.

Note: We can copy the asterisk.pem, ca.crt to another folder before making the IP phone's certificate.

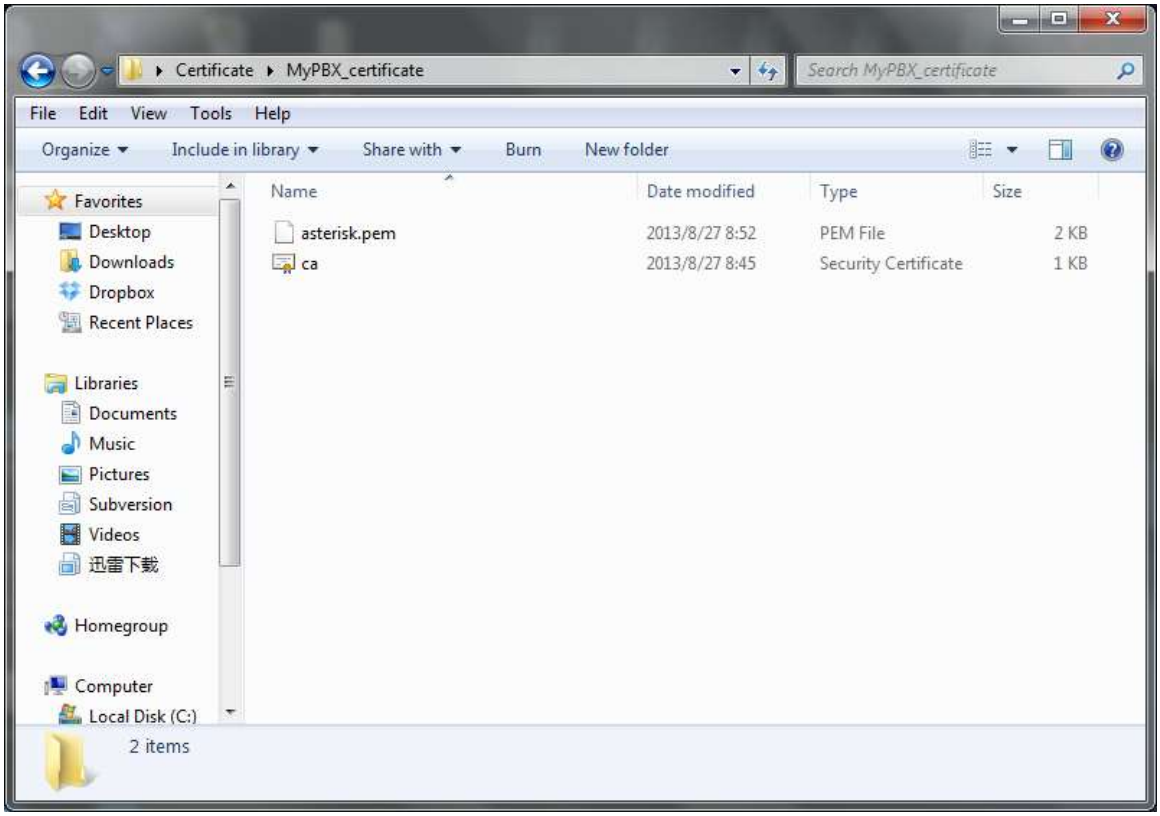


Figure I-11

Step3. Prepare the IP phone's certificate, ca.crt

Double click "ca.bat", input the information of IP phone step by step.

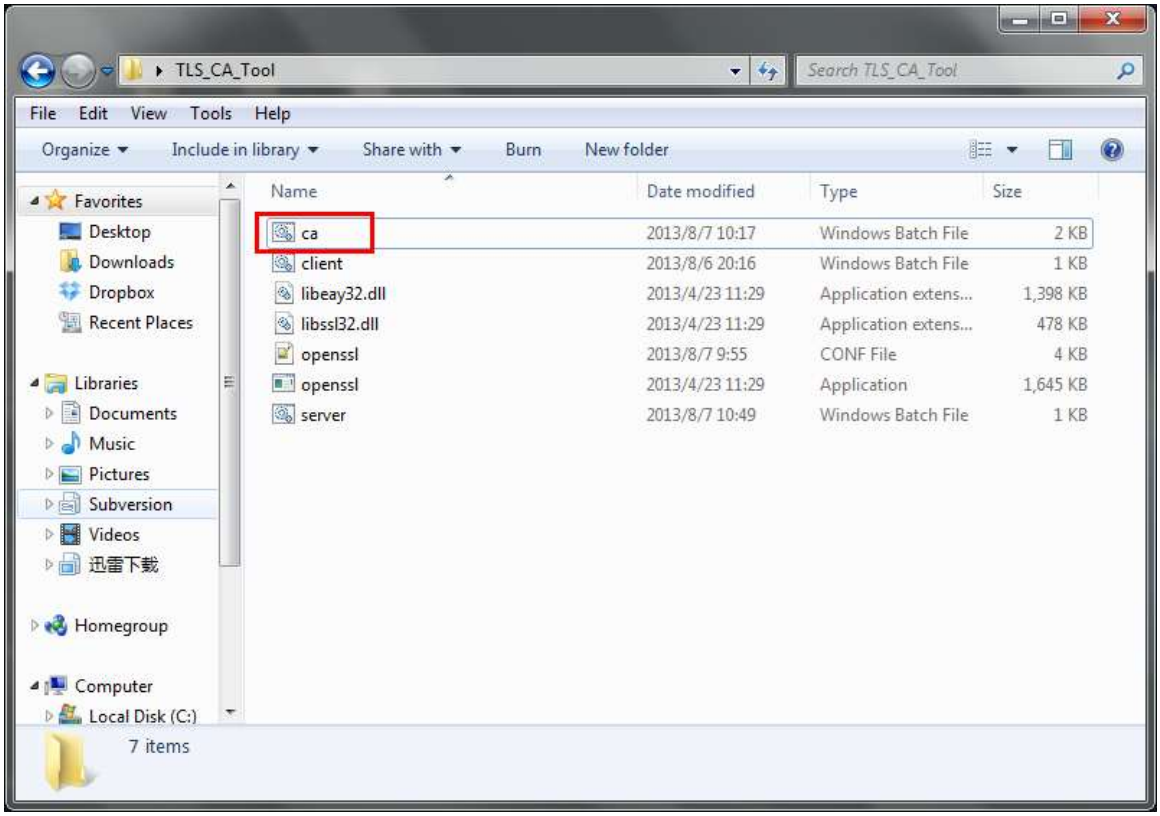


Figure I-12

In this example, the IP phone's IP address is 192.168.4.71.

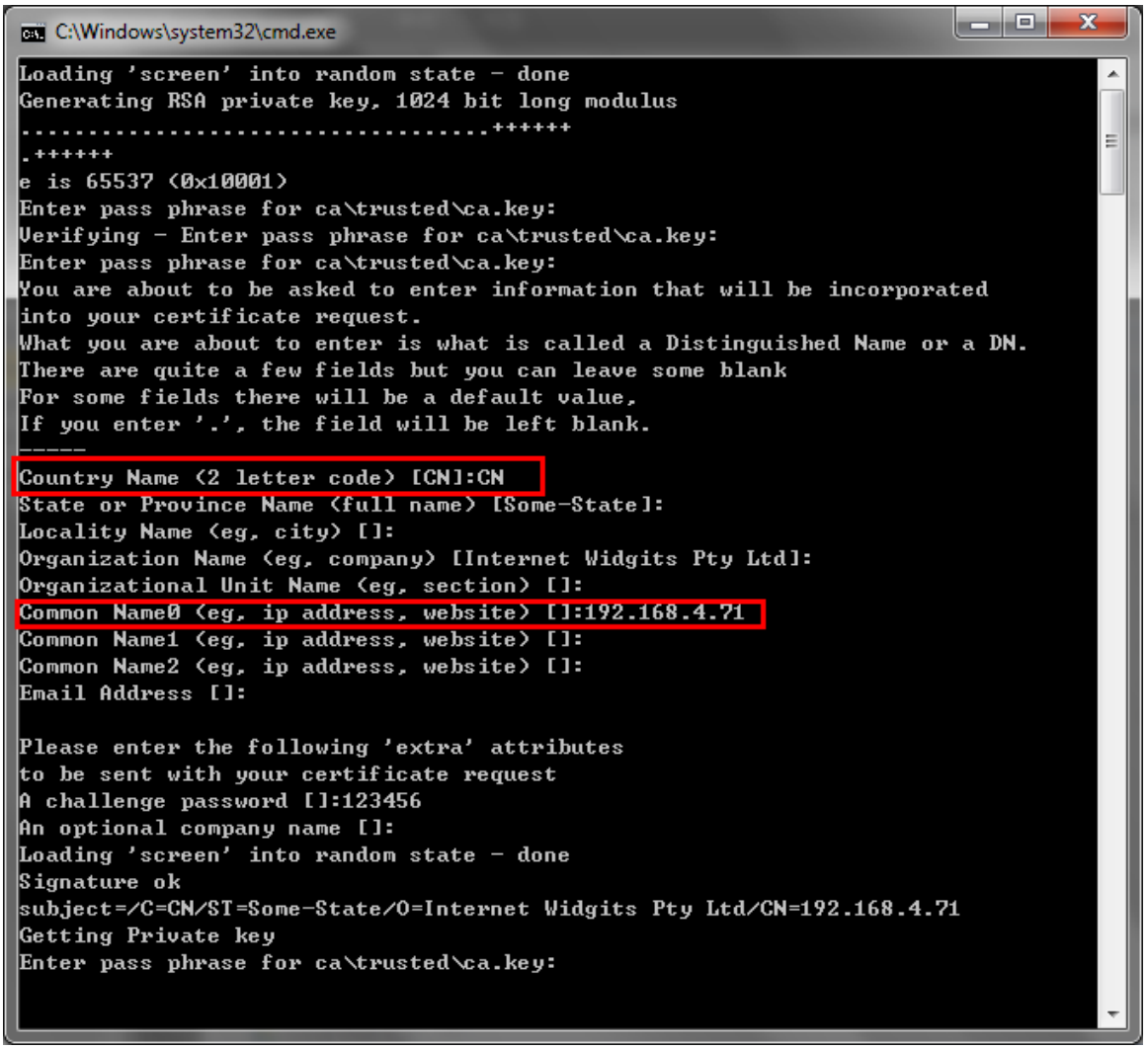


Figure I-13

When done, we can find the ca.crt in this folder.

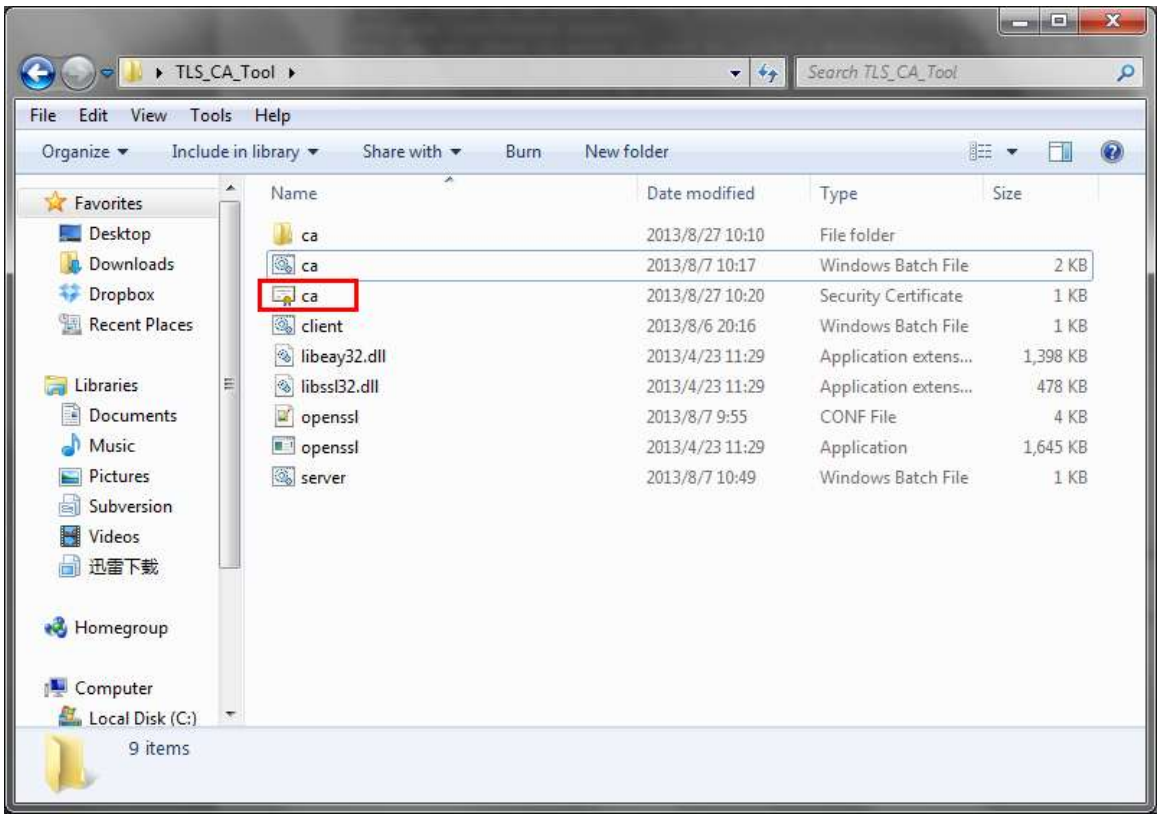


Figure I-14

The ca.crt in folder /TLS_CA_Tool/ca/trusted is the same as the above one.

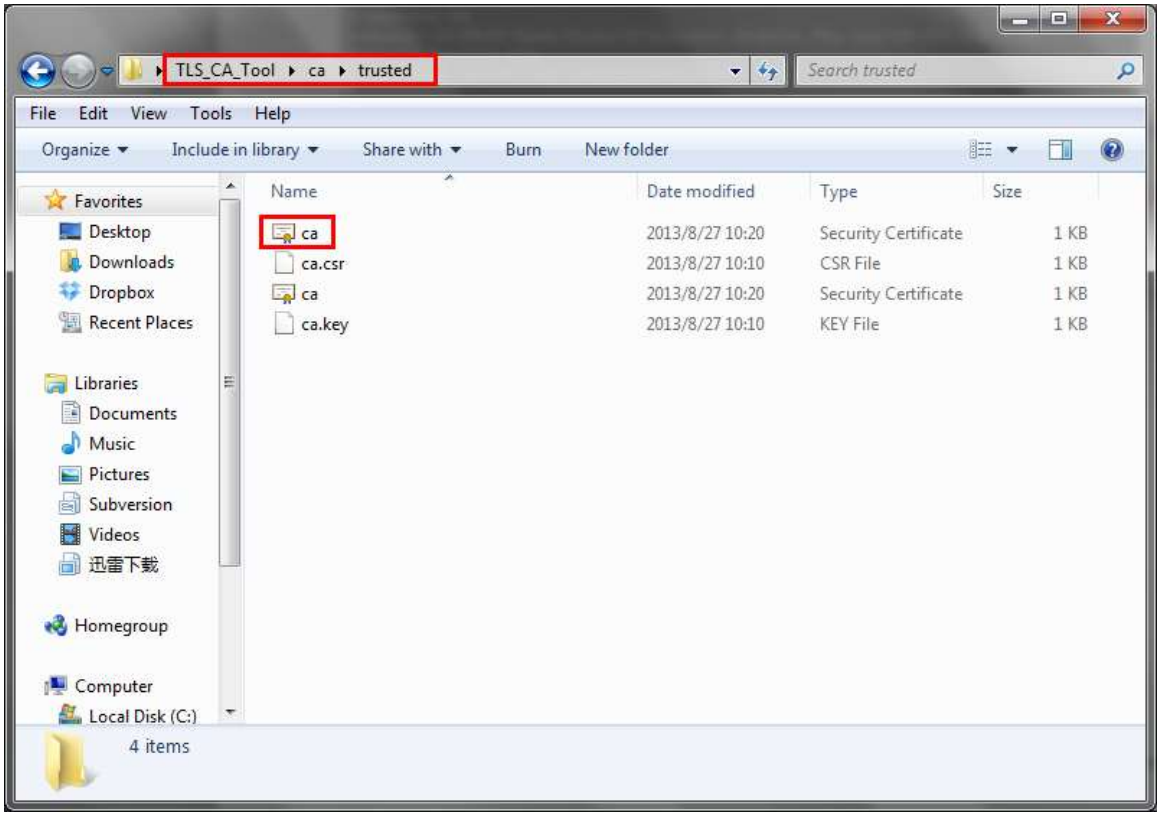


Figure I-15

The IP phone's certificate is finished.

Note: If you have got your own CA for IP phone, you can rename it to CA.crt and copy it

to folder "/TLS_CA_Tool/ca/trusted" before making the "client.pem".

Step4. Prepare "client.pem", the "IP phone's server certificate".

Double click "client.bat".

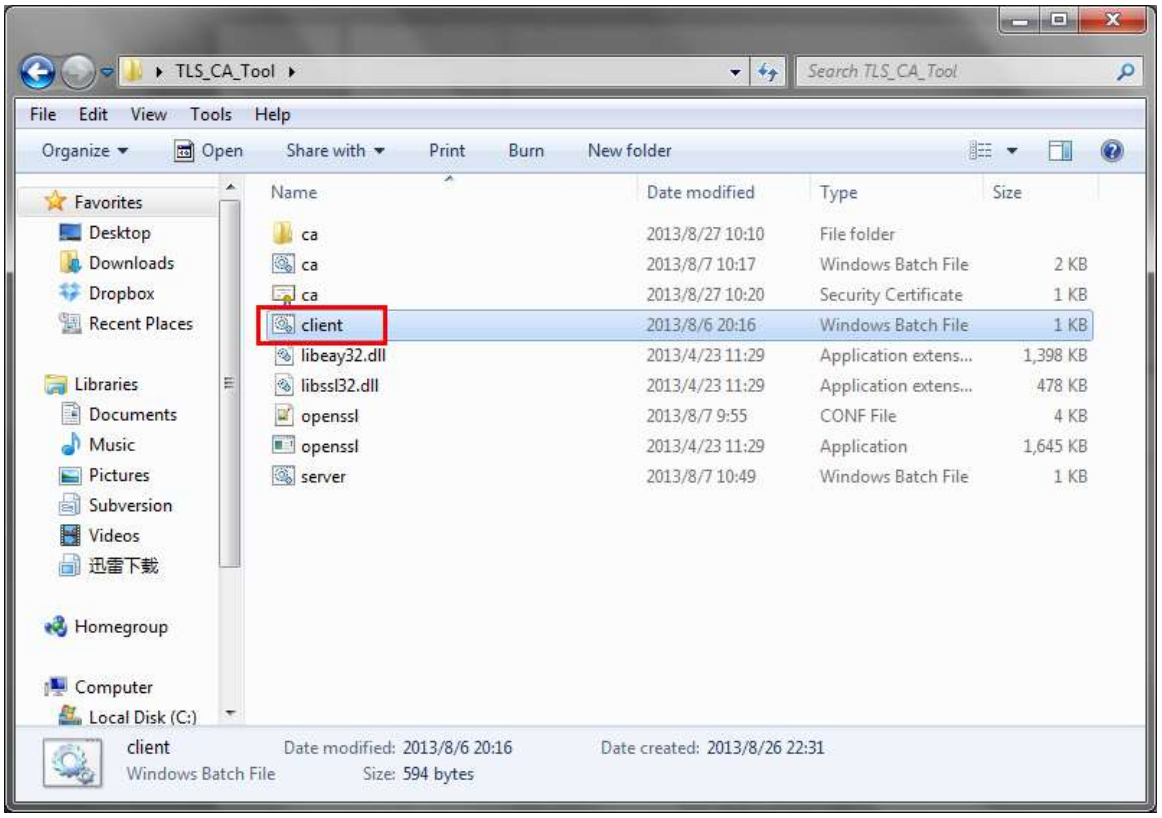
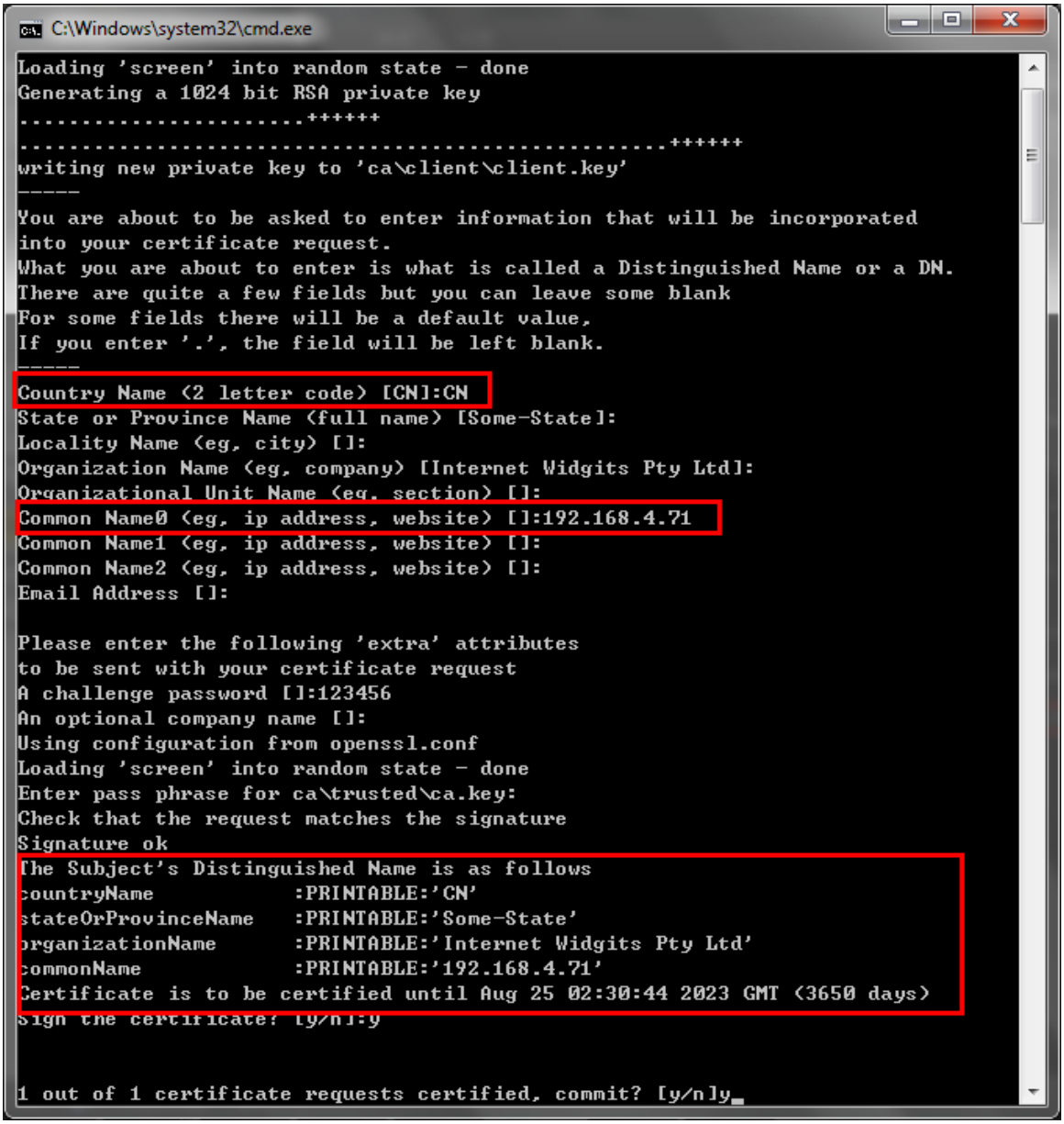


Figure I-16

Input the IP phone's information step by step in this script; make sure the content is the same as Step3.


C:\Windows\system32\cmd.exe
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'ca\client\client.key'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [CN]:CN
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name0 (eg, ip address, website) []:192.168.4.71
Common Name1 (eg, ip address, website) []:
Common Name2 (eg, ip address, website) []:
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:
Using configuration from openssl.conf
Loading 'screen' into random state - done
Enter pass phrase for ca\trusted\ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName :PRINTABLE:'CN'
stateOrProvinceName :PRINTABLE:'Some-State'
organizationName :PRINTABLE:'Internet Widgits Pty Ltd'
commonName :PRINTABLE:'192.168.4.71'
Certificate is to be certified until Aug 25 02:30:44 2023 GMT (3650 days)
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y

Figure I-17

Confirm all the information we input before clicking "y" to finish this guide.

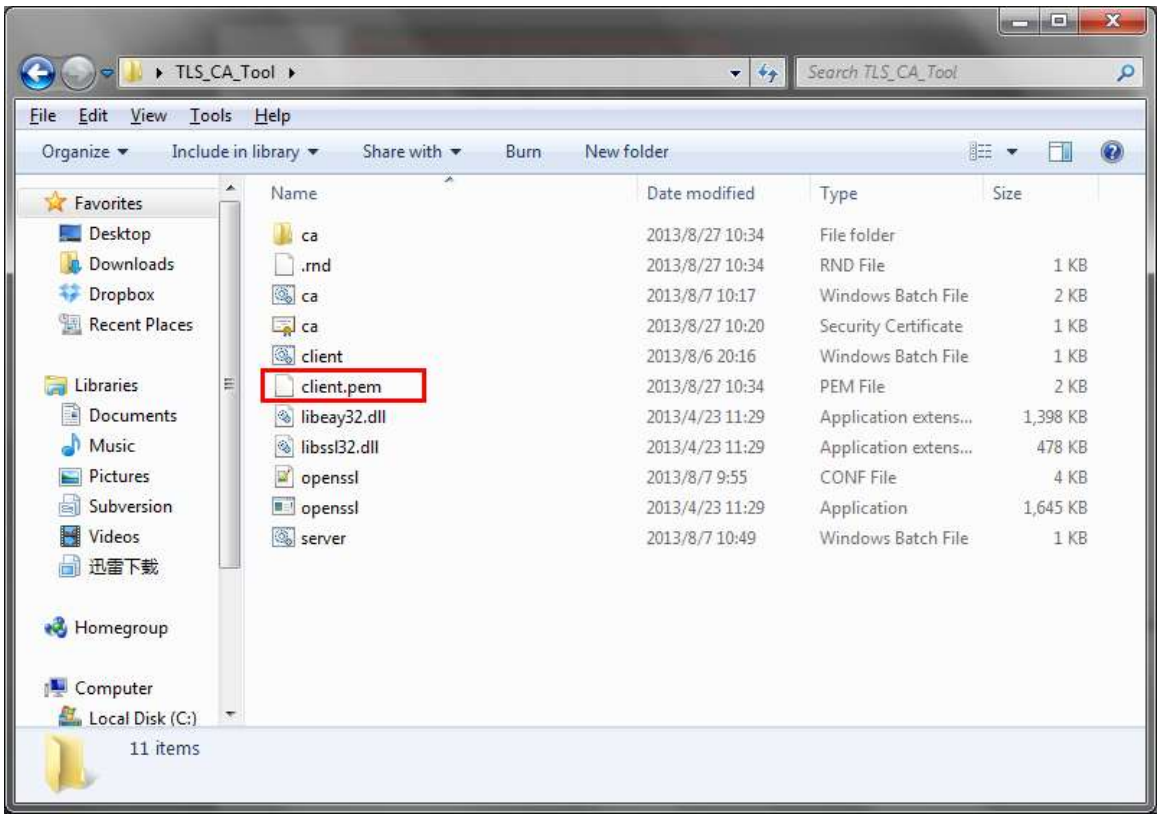


Figure I-18

The "IP phone's server certificate" is ready.

Note: We can copy the client.pem, ca.crt to another folder before uploading.

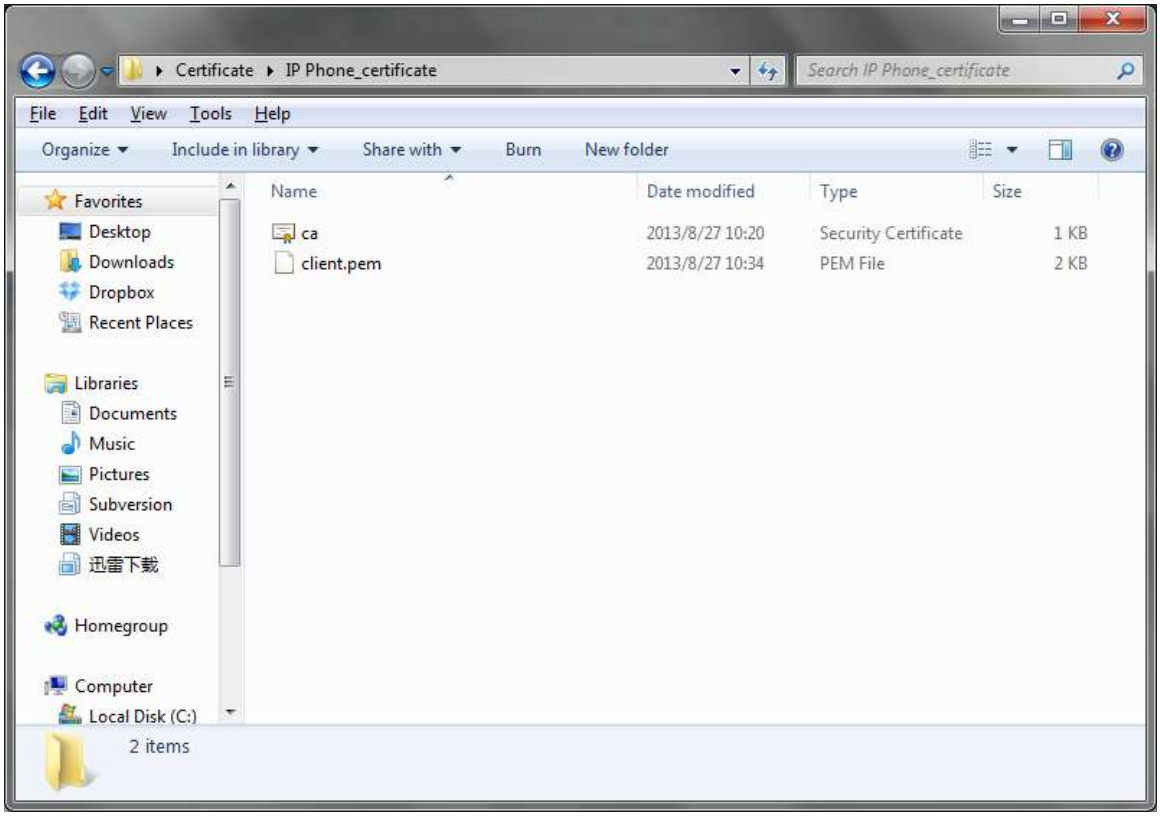


Figure I-19

All the certificates are prepared.

3. Upload certificates

3.1 Upload IP phone's certificates

In this example, IP phone's model is Yealink T28.

Step1. Upload "IP phone's server certificate" (client.pem).

Click "Security→Server Certificates" to upload client.pem

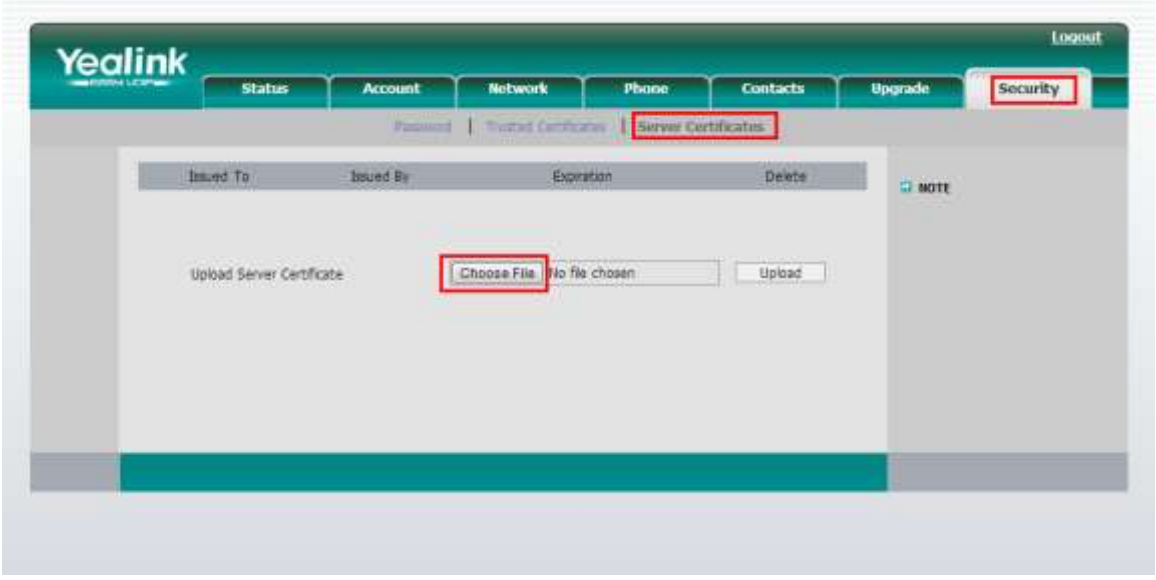


Figure I-20

Click "Choose File" and upload IP phone's server certificate. IP phone will reboot by itself when uploaded successfully to take effect.

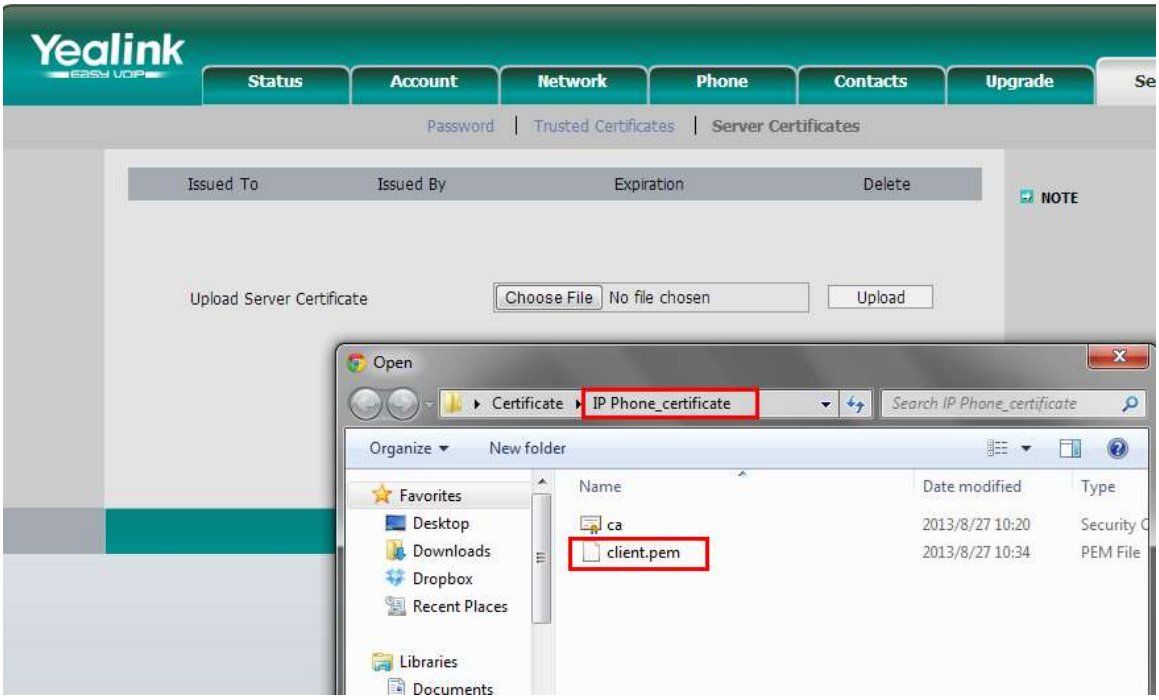


Figure I-21

When IP phone boots up again, we can check the certificate status.

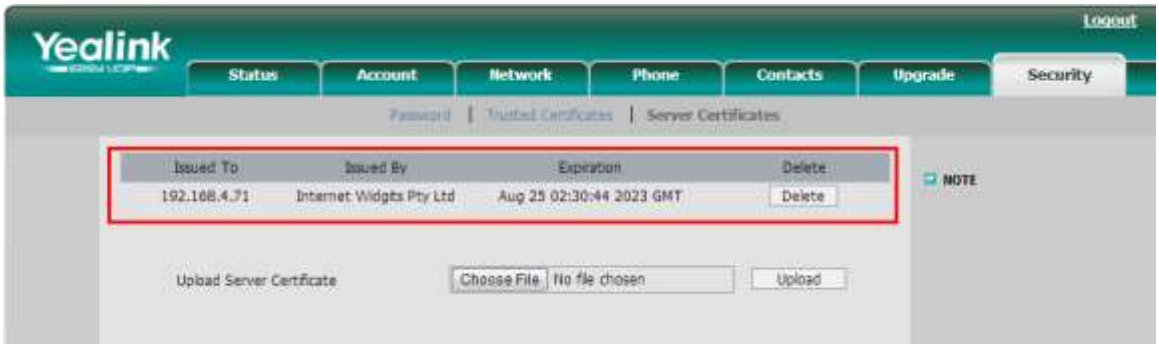


Figure I-22

Step2. Upload the trusted certificate.

The trusted certificate is the ca.crt of MyPBX. It will be sent to MyPBX during the registry process for authorization.

Click "Security→Trusted Certificates", upload MyPBX's ca.crt.

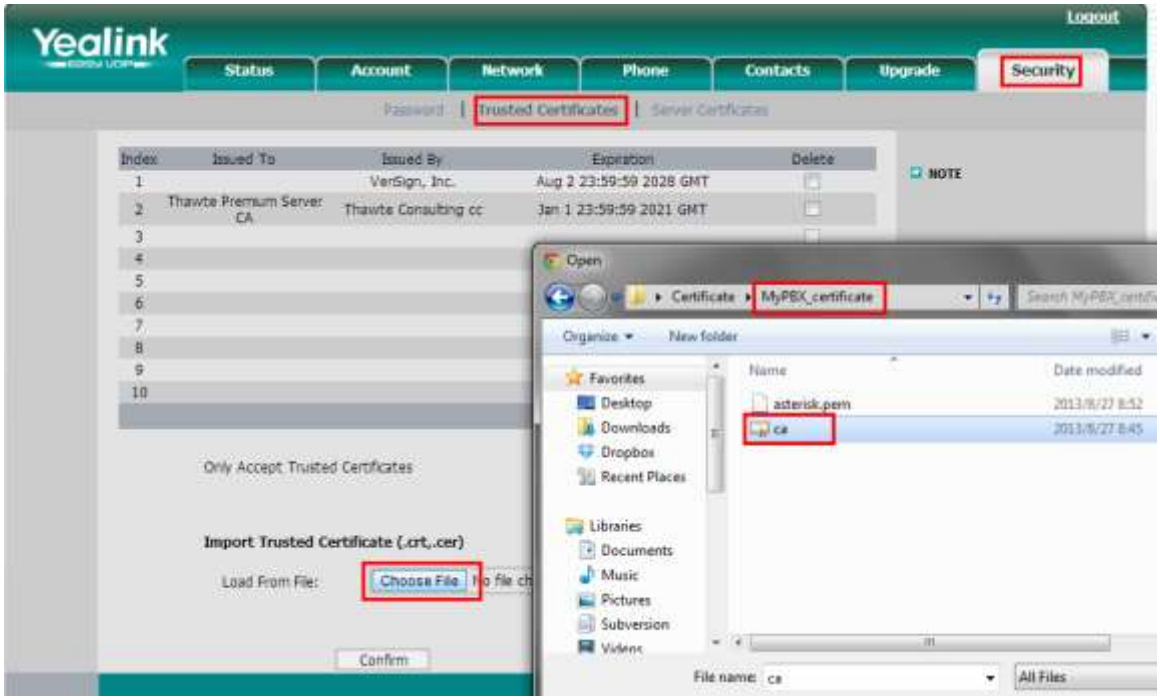


Figure I-23

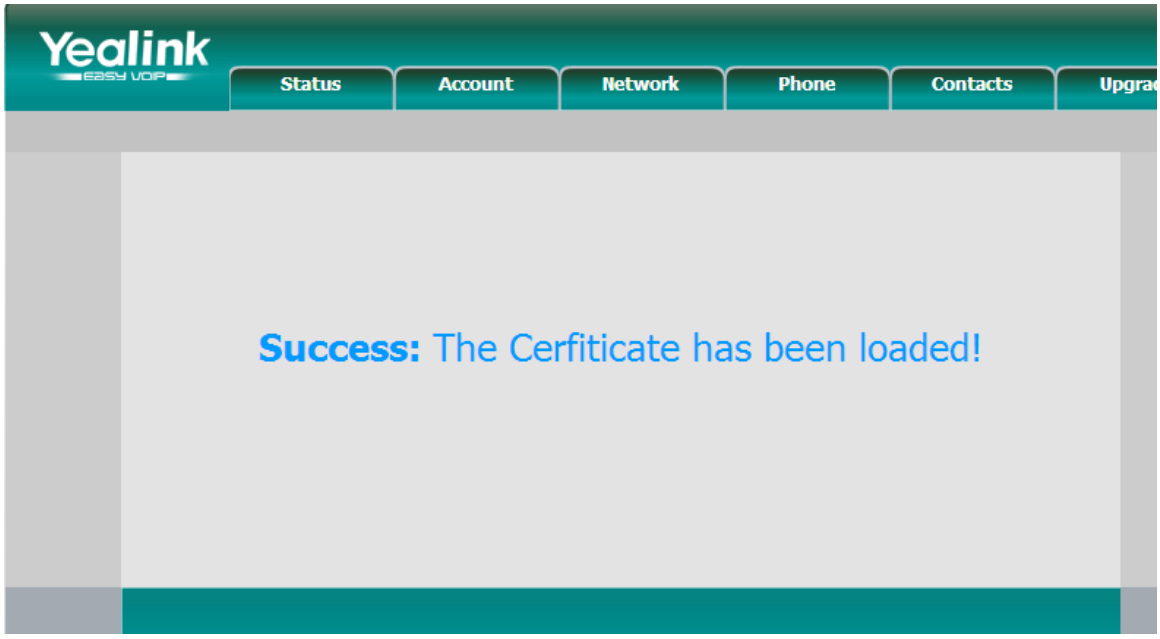


Figure I-24

When done, we can check the content of CA.crt like the picture shown below.

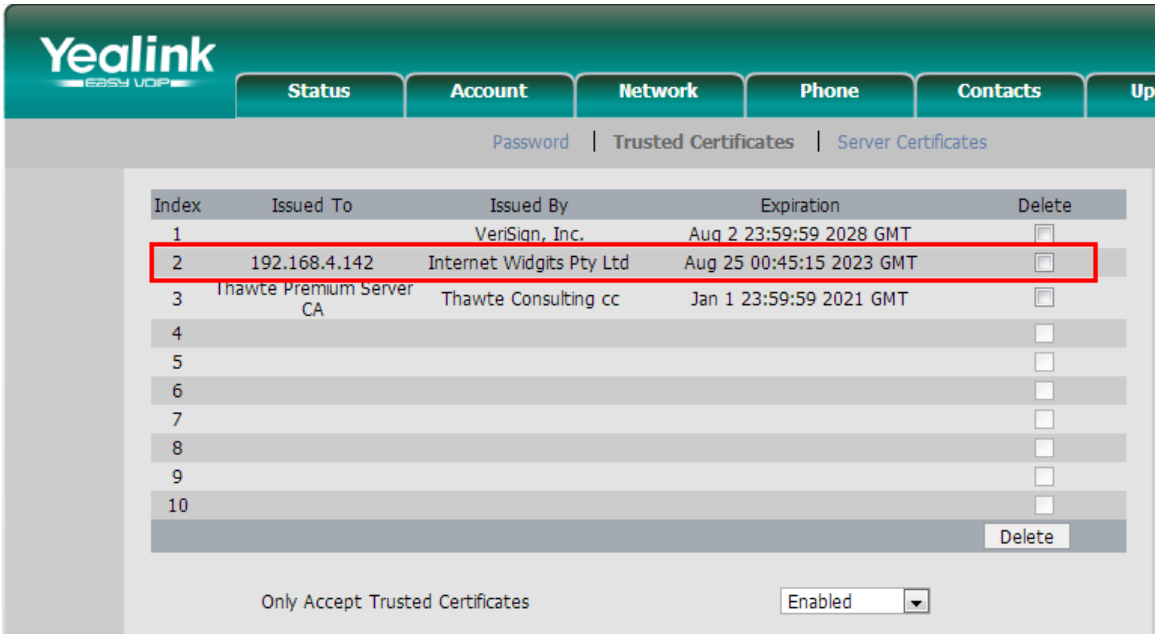


Figure I-25

The certificates in IP phone side are well uploaded.

3.2 Upload MyPBX's certificates

In this example, the model of MyPBX is MyPBX U200 (firmware version: 15.18.0.22)

Step1. Upload MyPBX's server certificate (asterisk.pem)

Click "PBX->Advanced Settings->Certificates", then click "Upload Certificates", choose "PBX Certificates" in Type windows, then upload the asterisk.pem.

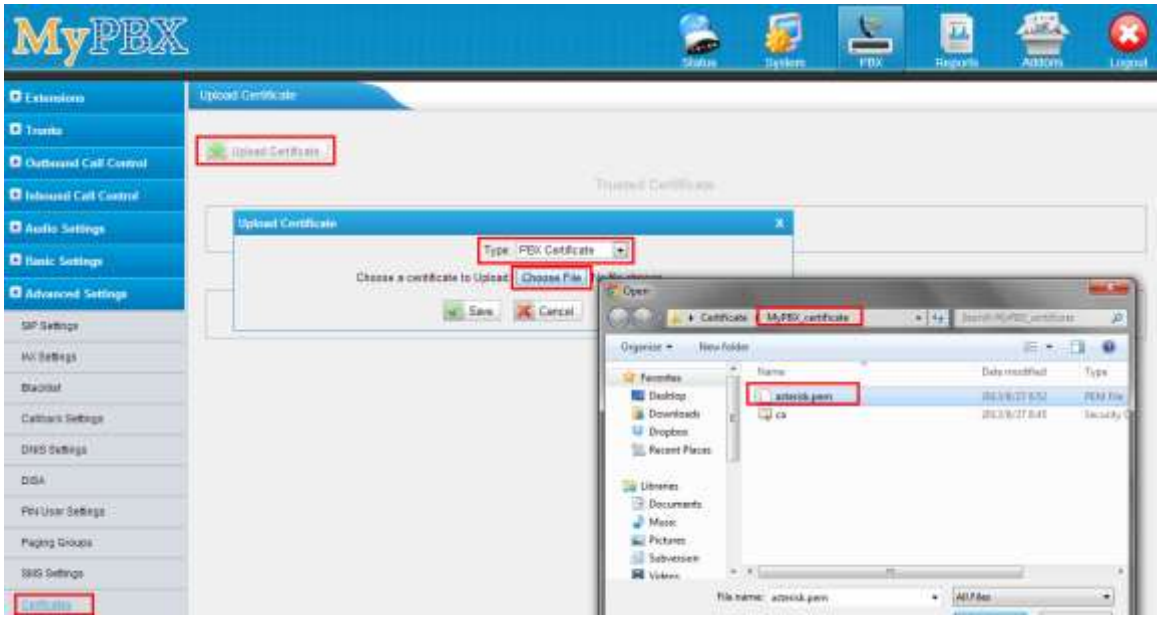


Figure I-26

Click Save to upload, you will need to reboot MyPBX to take effect.

Figure I-27

Click "Reboot Now" to reboot MypBX. When done, we can move to Step 2.

Figure I-28

Step2. Upload the trusted certificate.

The trusted certificate in MyPBX should be the ca.crt of IP phone.
Click "Upload Certificates" and choose "Trusted Certificates" in Type windows, then upload the IP phone's ca.crt.

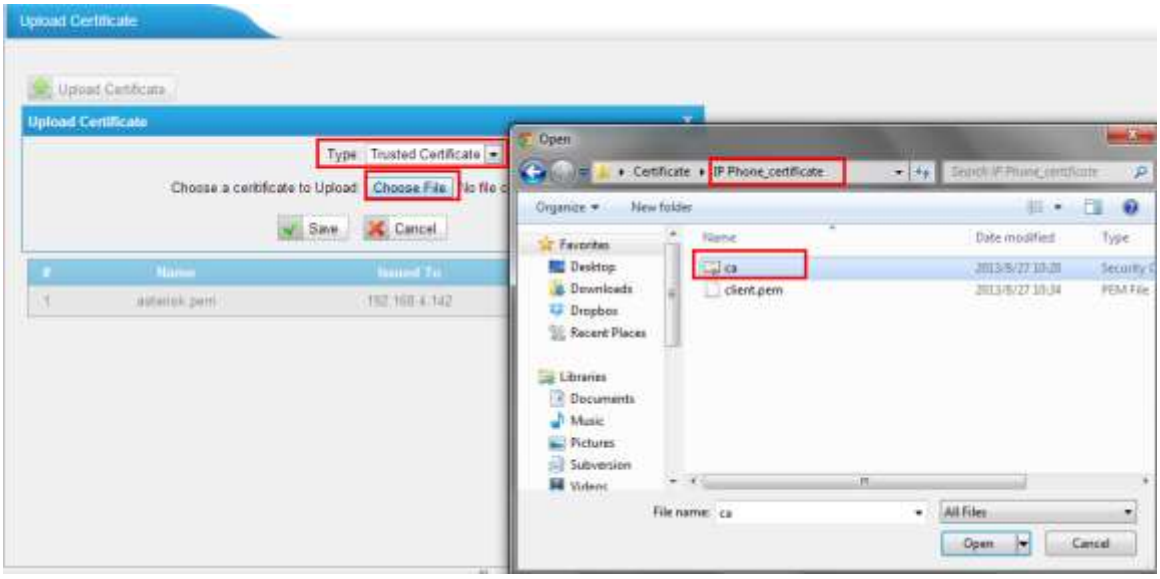


Figure I-29

Click "Save" to upload, then click "Apply Changes".

Figure I-30

The certificates in MyPBX side are well uploaded.

4 Register IP phone to MyPBX via TLS

Before registering IP phone to MyPBX, we need to create a SIP extension in MyPBX side in advance, or edit the existing one. In this example, extension number is 303.

We need to set TLS protocol in this page, click save and "Apply Changes" on Web.

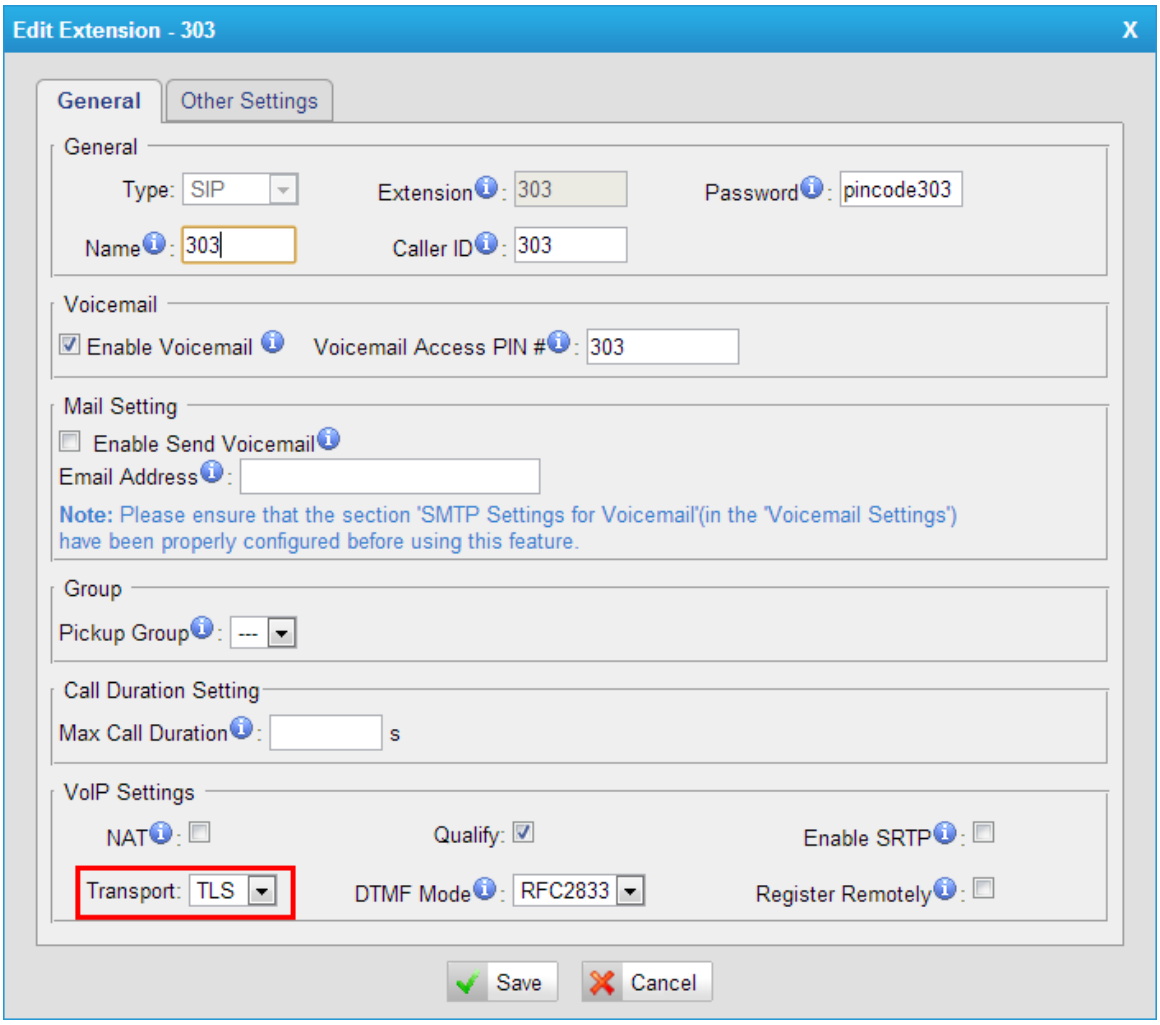


Figure I-31

Open IP phone's configuration page, input the registry information of extension 303.

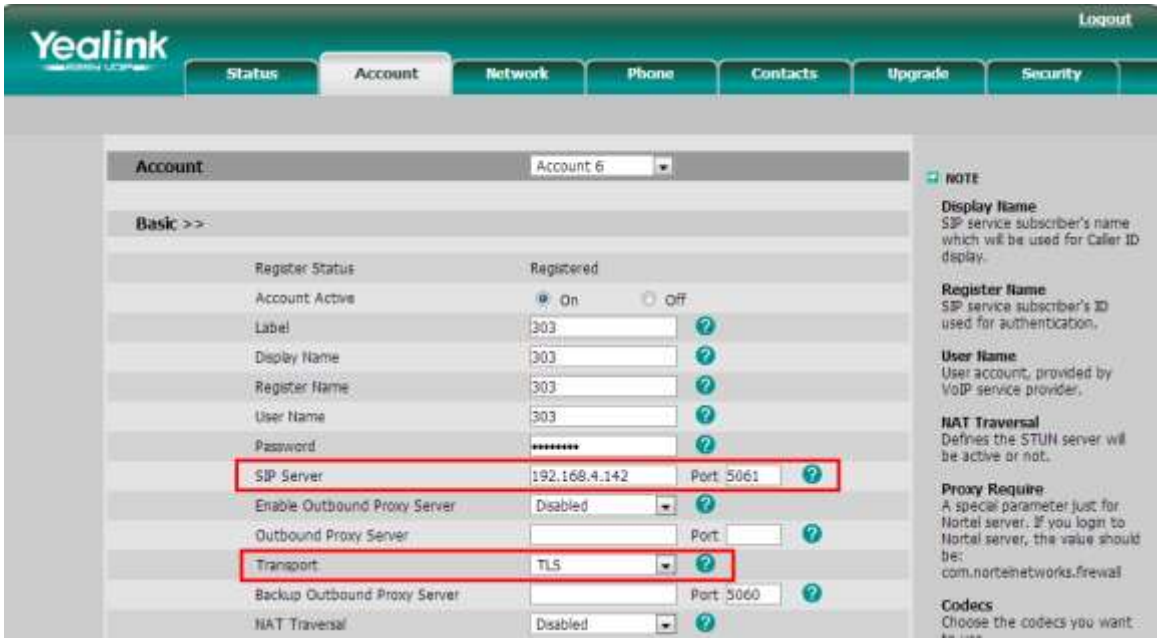


Figure I-32

Click "Confirm" to apply the changes, then extension 303 is registered via TLS.
We can also check the status in "Extension Status" page of MyPBX.

Figure I-33

If you have any problems about extension's registry, please run a packet trace in "Reports→System Logs→Packet Capture Tool", input IP phone's IP address, choose the eth port, then click "Start". You can register the IP phone again, then click "Stop" and download the package to analyze via wireshark. You can also send it to us for analyzing.

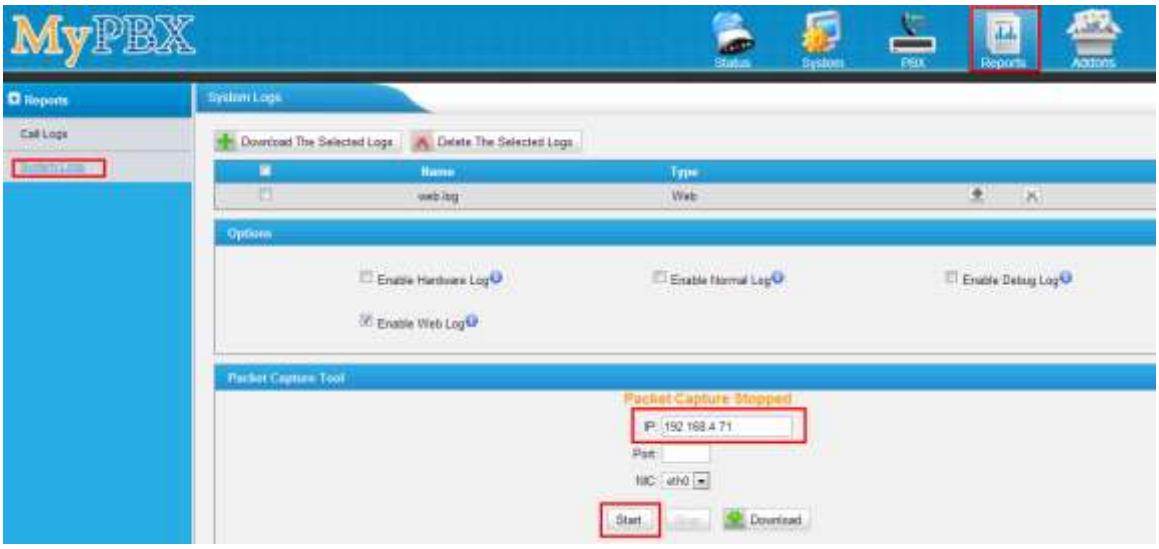


Figure I-34

I.2 How to register SIP trunk to VoIP provider via TLS

If you have got the SIP trunk from provider that is using TLS, we can configure it in MyPBX and choose TLS within the trunk, here are two examples for you.

VoIP trunk:

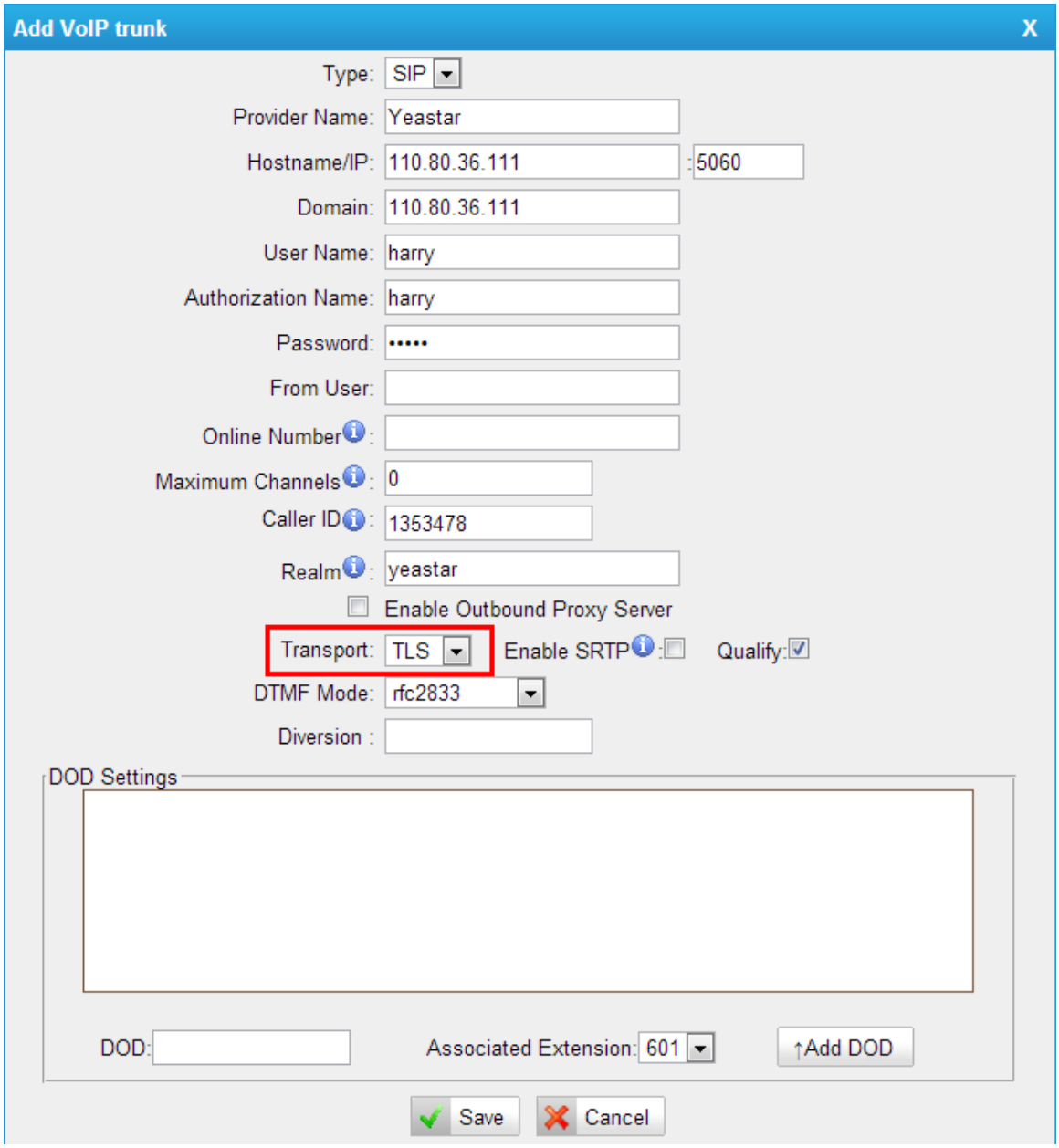


Figure I-35

Service provider trunk (P-P).

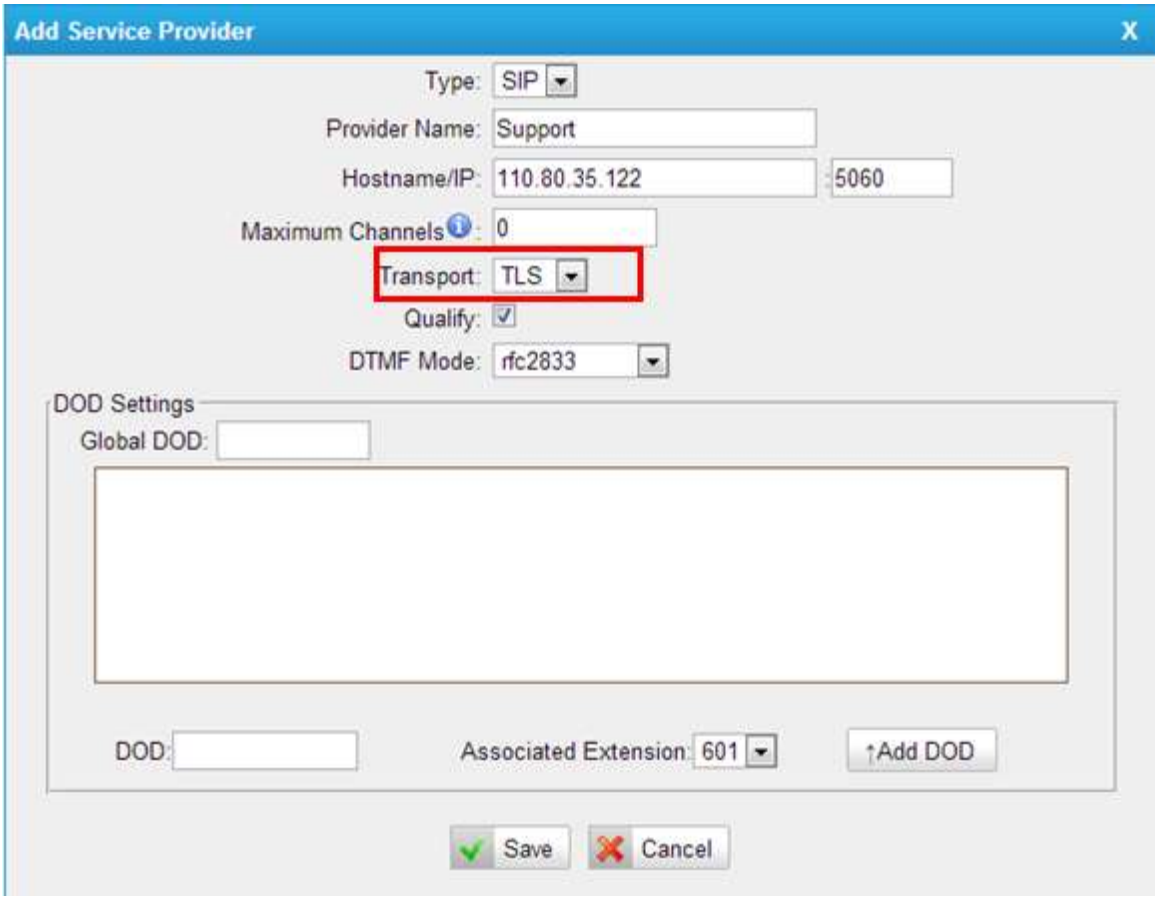


Figure I-36

If you have got problem when registering to provider via TLS, you can also run a packet trace in "System Log" page using "Packet Capture Tool", then send it to provider or us to analyze.

[Finish]